# SnapGear™ VPN Appliance Family
# User Manual

Rev: 1.8.4
September 10th, 2003

SnapGear, Inc.
7984 South Welby Park Drive #101
Salt Lake City, Utah 84084
Email: support@snapgear.com
Web: www.snapgear.com

# Table of contents


**1. Introduction ..... 1**
SnapGear gateway appliances ..... 1
SnapGear PCI appliances ..... 2
Document conventions ..... 4
Your SnapGear gateway appliance ..... 5
SnapGear gateway appliance features ..... 8
Your SnapGear PCI appliance ..... 10
**2. Getting started ..... 12**
SnapGear gateway appliances ..... 12
Configuring the SnapGear appliance on your network ..... 15
SnapGear Quick Setup ..... 21
Setup PCs to access the Internet ..... 25
SnapGear PCI appliances ..... 30
**3. Connecting to the Internet ..... 35**
Physically connect modem device ..... 35
Select Internet connection ..... 36
Internet failover ..... 40
Configure PCs to use SnapGear appliance Internet gateway ..... 43
Establishing the connection ..... 46
**4. Network Setup and DMZ ..... 47**
Connections ..... 47
DMZ Configuration ..... 50
Load balancing ..... 51
Routes ..... 51
Advanced ..... 51
**5. Dial-in server configuration ..... 52**
Dial-in setup ..... 54
Dial-in user accounts ..... 57
Remote user configuration ..... 60
**6. Network configuration ..... 66**
IP configuration ..... 66
Advanced IP configuration ..... 69
DHCP server ..... 71
Advanced networking ..... 77

**7. Firewall ..... 78**
Incoming access ..... 78
Packet Filtering ..... 83
Firewall rules ..... 88
Intrusion detection and blocking ..... 89
Content filtering ..... 92
**8. Virtual Private Networking ..... 95**
PPTP client setup ..... 96
PPTP server setup ..... 98
IPSec setup ..... 111
Configuring the branch office SnapGear appliance ..... 111
Configuring the headquarters SnapGear appliance ..... 126
Tunnel List ..... 130
NAT Traversal Support ..... 134
Dynamic DNS Support ..... 134
Certificate Management ..... 135
Troubleshooting ..... 141
GRE ..... 145
L2TP ..... 147
**9. System ..... 149**
Date and Time ..... 149
Users ..... 150
Diagnostics ..... 153
Advanced ..... 154
**10. Technical support ..... 157**
**Appendix A – LED status patterns ..... 158**
**Appendix B – Terminology ..... 159**
**Appendix C – System Log ..... 166**
Access Logging ..... 166
Creating Custom Log Rules ..... 168
Rate Limiting ..... 171
Administrative Access Logging ..... 171
Boot Log Messages ..... 172

# 1. Introduction

This chapter provides an overview of your SnapGear appliance's features and capabilities, and explains how to install and configure your SnapGear appliance.

This manual describes how to take advantage of the features of your SnapGear appliance, including setting up network connections, a secure firewall and a VPN. It also describes how to set up the SnapGear appliance on your existing or new network using the SnapGear Management Console web administration pages.

## SnapGear gateway appliances

The SnapGear gateway appliance (LITE2, LITE2+, SOHO+, PRO, PRO+, SME530, SME550, SME570, SME575) enables your office LAN to share a single, secure Internet connection.

The SnapGear appliance provides Internet security and privacy of communications for small and medium enterprises. It simply and securely connects your office to the Internet, and with its robust stateful firewall, shields your computers from outside threats. The SnapGear appliance checks and filters data packets to prevent unauthorized intruders gaining access.

The SnapGear appliance's NAT/masquerading firewall means that although computers on your office network can see and access resources on the Internet, all outsiders see is the SnapGear gateway appliance's external address.

SnapGear appliance models SME570 and SME575 have an additional Ethernet port that may be configured as a physically separate DMZ to host servers accessible to the outside world, in order to further secure your local network. Alternatively, it may be configured as a second Internet connection to perform network load balancing.

The SnapGear appliance provides you with a Virtual Private Network (VPN) server. A VPN enables remote workers or branch offices to securely access your company network to send and receive data at a very low cost. With the SnapGear appliance, you can remotely access your office network securely using the Internet. The SnapGear appliance can also connect to external VPNs as a client.

The following figure shows how your SnapGear appliance interconnects. If you are using the SnapGear LITE2+, a secondary hub/switch is not required as this unit has a 4-port Ethernet switch.

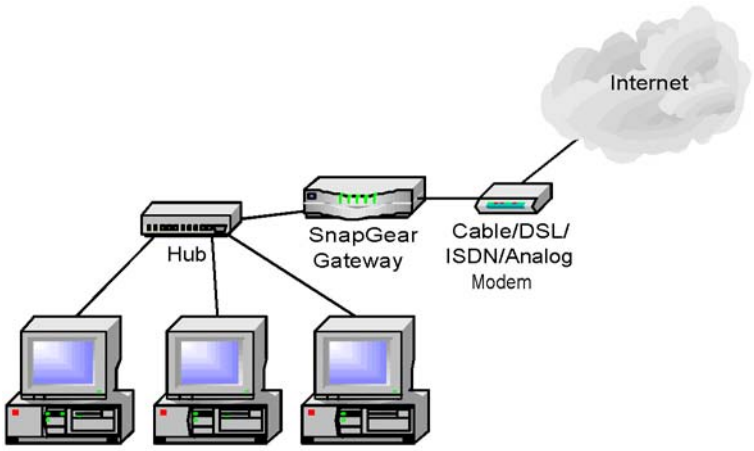



**Figure 1.1 SnapGear gateway appliance interconnection**

# SnapGear PCI appliances

The SnapGear PCI appliance (PCI630) is a hardware-based firewall and VPN server embedded in a 10/100 Ethernet PCI network interface card (NIC). It is installed into the host PC like a regular NIC, providing a transparent firewall to shield the host PC from malicious Internet traffic, and VPN services to allow secure remote access to the host PC.

This appliance is recommended for:

- Security conscious businesses that wish to separate firewall and VPN issues from server/desktop operating systems.
- Businesses that wish to eliminate the "soft center".
- For environments where the integrity of the host server operating environment cannot be controlled or trusted.

Unlike SnapGear gateway appliances, a single SnapGear PCI appliance it is not intended as a means for your entire office LAN to be connected to, and shielded from, the Internet. Installing a SnapGear appliance in each network connected PC gives it its own independently manageable, enterprise-grade VPN server and firewall, running in isolation from the host operating system.

This approach offers an increased measure of protection against internal threats as well as conventional Internet security concerns. You can update, configure and monitor the firewall and VPN connectivity of a workstation or server from any web browser. In the event of a breach, you have complete control over individual PCs' access policies independent of the host PC's operating system, even if the system has been subverted and is denying normal administrator access.

All network filtering and what can be CPU intensive cryptographic processing is handled entirely by the SnapGear appliance. This has the advantage over the traditional approach of a host-based personal software firewall and VPN services of not taxing the host PC's resources.

## Bridged mode

By default, the SnapGear PCI appliance operates in bridged mode. This is distinctly different from the NAT/masquerading behavior of the SnapGear gateway appliance range.

In bridged mode, the SnapGear appliance uses two IP addresses. Note that these addresses are both in the same range as the LAN, as no NAT/masquerading is being performed (see Chapter 7, *Firewall* for more information).

One IP address is used to manage the SnapGear appliance via the SnapGear management console web administration pages.

The other is the host PC's IP address, configurable through the host operating system identical to a regular NIC. This is the IP address that other PCs on the LAN see. It should be dynamically (DHCP) or statically configured to use the same gateway, DNS, etc. settings as a regular PC on the LAN.

It is possible to configure the SnapGear appliance to run in NAT mode. This is discussed in Chapter 6, *Network Configuration*.

## Secure by default

By default, the SnapGear appliance runs a fully secured stateful firewall. This means from the PC that it is plugged into, most network resources are freely accessible. However, any services that the PC provides, such as file shares or web services (e.g. IIS) will *not* be visible to the general office LAN without further configuration of the SnapGear appliance. For details on how services on the host PC can be made available to the general office LAN, see the section *Allowing individual ports in bridged mode* at the end of Chapter 7, *Firewall*.

| Step | Action | Chapter, Section |
|---|---|---|
| 1. | Interconnect the SnapGear appliance and PC on your LAN | Chapter 2, *Getting Started* |
| 2. | Setup SnapGear appliance's initial LAN IP address | Chapter 2, *Configuring the SnapGear appliance on your network* |
| 3. | Quick Setup of SnapGear appliance's LAN port and Internet connection | Chapter 2, *Quick Setup* |
| 4. | Setup PCs on your LAN for the Internet (*SnapGear gateway appliance only*) | Chapter 2, *Setup PCs to access the Internet* |

**For more details..**

| | |
|---|---|
| Connecting the mode for Internet access | Chapter 3, *Connecting to the Internet* |
| Setting up Internet account and establishing connection | Chapter 3, *Connecting to the Internet* |
| Setup or modify SnapGear appliance services | Chapter 5, *Dial-in Server*<br>Chapter 7, *Firewall*<br>Chapter 8, *Virtual Private Networking* |

Installing your SnapGear appliance into a well-planned network is quick and easy. Although network planning and design is outside the scope of this manual, please take the time to plan your network prior to installing your SnapGear appliance.

## Document conventions

This document uses different fonts and typefaces to show specific actions.

***Warning***

*Warning text like this highlights important issues.*

**Bold text** in procedures indicates text that you type, or the name of a screen object (e.g. a menu or button).

# Your SnapGear gateway appliance

SnapGear gateway appliances include:

- LITE2
- LITE2+
- SOHO+
- PRO
- PRO+
- SME530
- SME550
- SME570
- SME575

The following items are included with your SnapGear gateway appliance:

- Power adaptor
- Installation CD
- Printed Quick Install guide
- Cabling including
    - 1 normal *straight through* UTP cable (blue color).
    - 1 *crossover* UTP cable (either gray or red color). If you have the LITE2+ you will receive two straight through cables (blue color).

## Front panel LEDs

The front and rear panels contain LEDs indicating status. An example of the front panel LEDs are illustrated in the following figure and detailed in the following table.

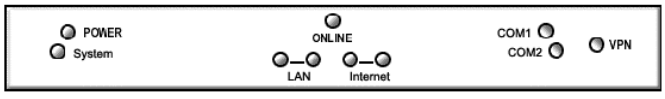



**Figure 1.2 SnapGear SOHO+/PRO front panel LEDs**

***Note***

*Not all the LEDs described below are present on all SnapGear appliance models. Also, labels vary from model to model.*

| Label | Activity | Description |
|---|---|---|
| *Power*<br>*PWR* | On | Power is supplied to the SnapGear appliance |
| *System*<br>*Heart Beat*<br>*TST* | Flashing | The SnapGear appliance is operating correctly |
| | On | If this LED is on and not flashing, an operating error has occurred |
| *LAN Link*<br>*LAN Lnk* | On | A cable is connected correctly to another device (e.g. a hub) |
| *Internet Link*<br>*WAN Lnk* | On | A cable is connected correctly to another device (e.g. a cable modem) |
| *LAN Activity*<br>*LAN Act*<br>*LAN* | Flashing | Network traffic on the LAN network interface |
| *Internet Activity*<br>*WAN Act*<br>*WAN Activity*<br>*WAN* | Flashing | Network traffic on the Internet network interface |
| *DMZ Activity* | Flashing | Network traffic on the DMZ network interface |
| *COM1/COM2*<br>*Serial Activity*<br>*TX/RX*<br>*Modem* | Flashing | For either of the SnapGear appliance COM ports, these LEDs indicate receive and transmit data |
| *Online* | On | A valid Internet connection is present |
| *VPN* | On | Virtual Private Networking is enabled |

## Rear panel

The rear panel contains the connector ports for the LAN, Internet (*Internet*/*WAN*), DMZ (SME570, SME575 only) and modem (*COM1*, *COM2*), LAN status LEDs, Internet status LEDs, the reset button and power inlet.

Additionally, the SnapGear PRO+ has an RJ11 phone jack (*Modem*) to connect a phone line to its internal modem.

For units with LAN/Internet status LEDs, the lower LED indicates the *link* condition, where a cable is connected correctly to another device. The upper LED indicates *network activity*.

# SnapGear gateway appliance features

## Internet link features

- 10/100baseT Ethernet port (Internet/WAN) that connects to the Internet using a cable or ADSL modem (10BaseT on other PRO, SOHO+, LITE2, LITE2+).
- Serial port to attach an external modem or ISDN TA. PRO and SOHO+ models have two serial ports. PRO+ models have a single serial port and an internal modem.
- Front panel serial status LEDs (for TX/RX).
- Online status LEDs (for Internet/VPN).
- Rear panel Ethernet link and activity status LEDs (not on LITE2, LITE2+).

## LAN link features

- 10/100BaseT LAN port to connect to the local Ethernet network (10BaseT on PRO, SOHO+).
- Rear panel Ethernet link and activity status LEDs (not on LITE2, LITE2+).

## DMZ link features (SME570, SME575 only)

- 10/100BaseT DMZ port.
- Real panel Ethernet link and activity status LEDs.

## Dial-in connection features

An external modem may be attached via serial port for dial-in connections (not on LITE2, LITE2+). Additionally, the SnapGear PRO+ has an internal modem that can be used for dial-in connections.

Environmental features

- External power adaptor (voltage/current depends on individual model).
- Front panel operating status LEDs: Power, System/TST/Heart Beat.
- Operating temperature between 0° C and 40° C.
- Storage temperature between -20° C and 70° C.
- Humidity between 0 to 95% (non-condensing).

# Your SnapGear PCI appliance

SnapGear PCI appliances include:

- PCI630

The following items are included with your SnapGear PCI appliance:

- Installation CD
- Printed Quick Install guide

## LEDs

The rear panel contains LEDs indicating status. The two LEDs closest to the network port are network activity (upper) and network link (lower). The two other LEDs are power (upper) and heart beat (lower).

**Figure 1.3 SnapGear PCI630 LEDs**

| Label | Activity | Description |
|---|---|---|
| *Power* | On | Power is supplied to the SnapGear appliance. |
| *Heart beat* | Flashing | The SnapGear appliance is operating correctly. |
| *Network activity* | Flashing | Data is being transmitted or received. |
| *Network link* | On | The SnapGear appliance is attached to the network. |

## SnapGear PCI appliance features

### Network link features

- 10/100baseT Ethernet port that connects to the LAN (or Internet using a cable or ADSL modem).
- Ethernet LEDs (link, activity).

### Environmental features

- Status LEDs: Power, Heart Beat.
- Operating temperature between 0° C and 40° C.
- Storage temperature between -20° C and 70° C.
- Humidity between 0 to 95% (non-condensing).

# 2. Getting started

If you are setting up a SnapGear gateway appliance (LITE2, LITE2+, SOHO+, PRO, PRO+, SME530, SME550, SME570, SME575) proceed to *SnapGear gateway appliances* below. If you are setting up a SnapGear PCI appliance (PCI630), proceed to *SnapGear PCI appliances* towards the end of this chapter.

## SnapGear gateway appliances

Your SnapGear appliance provides a secure, simple gateway to connect PCs and other devices on your local network to the outside world. This chapter provides step-by-step instructions for connecting the SnapGear appliance to your LAN. The procedures in this section expand on the steps in the *SnapGear Quick Install Guide*, which you may prefer to use if you are in a hurry.

If you are connecting the SnapGear appliance to an established LAN, use a standard Ethernet cable to connect the SnapGear LAN port to a spare port on the network's hub. If you are connecting your SnapGear appliance to a single PC, use the provided Ethernet crossover cable to interconnect them directly. In the case of the SnapGear LITE2+, use a standard Ethernet cable to connect any one of its four LAN switch ports to a single PC, or an Ethernet crossover cable to connect to another hub.

The SnapGear appliance comes with an in-built DHCP server that can automatically assign IP addresses to other devices on the network. If you have an existing network, you may already have an active DHCP server and the PCs and devices on the network may already have IP addresses assigned. To simplify the installation in existing networks, the SnapGear appliance ships without an initial IP address and without the DHCP server activated by default.

If your network does not have an active DHCP server, it is recommended that you take advantage of using the SnapGear appliance as a DHCP server and setup the PCs on your network to dynamically receive TCP/IP configuration information.

Although it is not the default behavior, it is also possible to boot the SnapGear appliance with an initial, static IP address of **192.168.0.1** (netmask 255.255.255.0). While the SnapGear appliance is running (i.e. *System*/*TST*/*Heart Beat* is blinking), press the black *RESET* button twice within 3 seconds.

Note that this will reset any existing configuration options back to their factory defaults. Additionally, your network must (at least initially) be on the **192.168.0.0**/**255.255.255.0** subnet, as per step 6 of *New Networks*.

***Note***

*The following steps detail the initial setup procedure for networks with at least one Windows workstation. If you wish to perform the setup procedure using a Linux box, skip to the section called Initial setup using Linux later in this chapter.*

***Note***

*If you do not have an existing LAN, you need to configure one networked PC to get started:*

1. *Install an Ethernet adapter and software driver in at least one of the PCs to be networked.*

2. *Assign an IP address for your PC so the SnapGear appliance can be configured on the network. From the **Start** menu, select **Settings, Control Panel, Network** and click the **Configuration** tab (or **Protocols** if using NT).*

3. *Ensure that the TCP/IP networking protocol is installed. If not, click **Add** (then **Protocol** if using Windows 95/98, **Microsoft** then **TCP/IP**). Your PC will then reboot.*

4. *Highlight **TCP/IP** (followed by your Ethernet adapter's name if using 95/98) and click **Properties.***

5. *In the IP Address panel, select **Specify an IP Address**. Private network addresses should be in the ranges:*

   ```
   10.0.0.0 - 10.255.255.255  (10/8 prefix)
   172.16.0.0 - 172.31.255.255  (172.16/12 prefix)
   192.168.0.0 - 192.168.255.255 (192.168/16 prefix)
   ```

6. *If you plan to use the initial static IP feature of the SnapGear appliance, choose an address in the range:*

   ```
   192.168.0.0 - 192.168.0.255 (192.168.0/24 prefix)
   ```

   *Enter the value into the **IP Address** field followed by a number (1-254) to identify your PC (e.g.* 192.168.0.2*). You may have to reboot at this point.*

7. *Connect the SnapGear appliance's LAN port and the PC to the hub and continue with the following steps.*

***Note***

*Your SnapGear appliance ships with a Windows installation program called the* **SnapGear Setup Wizard**. *If you are using statically pre-assigned IP addresses on your network (i.e. there is a static network with no active DHCP server), the Setup Wizard will help assign an IP address to the SnapGear appliance.*

*On DHCP enabled (i.e. dynamic) networks , the Setup Wizard will locate the IP address assigned to your SnapGear appliance. The Setup Wizard will also provide the option to change the SnapGear appliance administrative password.*

*You can run the Setup Wizard from any PC on the network running Windows 2000, Windows XP, Windows ME, Windows NT 4 or Windows 95/98.*

*If you are using Windows 95 you must have the* MS Dial Up Networking 1.3 update *(**msdun13.exe**) installed.*

*If you are using an early version of Windows 95 (i.e. pre-OSR2), you must install the* Winsock 2.0 update *(**w95w2setup.exe**). If you are using Windows NT, Windows 2000, or Windows XP Professional you must be logged in as* administrator *to run the Setup Wizard.*

# Configuring the SnapGear appliance on your network

Below is an overview of the steps in initial setup of the SnapGear appliance on your network:

1. Apply power to the SnapGear appliance. When the SnapGear appliance is powered on in factory default mode, it has no LAN IP address. This state is indicated by all front panel LEDs except *Power* flashing (except on LITE2+). The LEDs remain flashing until a LAN IP address is acquired.

   ***Note***

   *If the LEDs on the front of the unit are not initially flashing, try pressing the* Reset/ERASE *button on the back panel of the unit. This does not apply to the LITE2+ model, which does not flash its LEDs. If after doing this all the LEDs on the front on the unit do not flash, then you may need to contact customer support.*

   *However, the SnapGear appliance may be acquiring an initial IP address from another DHCP server on the LAN, causing its LEDs to stop flashing soon after booting. In this case, the* SnapGear Setup Wizard *will detect this address, as detailed in the following steps.*

2. Insert the *Installation CD* into the CD drive of any Windows PC on your network that meets the system requirements. If the setup program does not run automatically, select **Run** from the **Start** menu and type **`z:\setup`** (where **`z`** is the letter of your CD drive).

3. Select the directory and Start menu group where the software utilities for your SnapGear appliance will be installed.

4. The wizard will search the network for your device. If your SnapGear appliance does not yet have an IP address assigned to it, you will be asked to enter one now. The next section, *Set up an IP address*, describes this scenario in more detail.

***Note***

*The front of the SnapGear appliance contains activity LEDs that vary slightly between models. These provide information on the operating status of your SnapGear appliance. In particular you should note:*

*The Power/PWR LED is on when power is applied (use only the SnapGear Power Adapter packaged with the unit).*

*The System/TST/Heart Beat LED blinks when the SnapGear appliance is running.*

*For all modes except the LITE2+, all LEDs (except Power/PWR) will flash when your SnapGear appliance is powered on for the first time. These LEDs stop flashing when the device has been assigned an IP address.*

## Set up IP addresses

To communicate on your network the SnapGear appliance will need an IP address. This is accomplished using the *SnapGear Setup Wizard* application that ships with your SnapGear CD.

***Note***

*The WAN interface is by factory default inactive in that there are no network services such as DHCP in operation, and no IP address is configured. The LAN interface is set up as a DHCP client, and will not initially have an assigned IP address. This is deliberately set to be passive so as not to interfere with your existing LAN. All of this will be configured later in the installation process but to get you up and running the* **setup.exe** *application is simply a miniature DHCP server that will give the SnapGear appliance a known IP address. If you use Linux, Unix, Macintosh or another operating system you should simply use a DHCP server application to assign an IP address.*

As the SnapGear appliance initially has no IP address, the front panel LEDs will be flashing.

The *SnapGear Setup Wizard* can be run from any PC on the network that is running Windows. To run SnapGear Setup Wizard:

Insert the *SnapGear Installation CD* into your CD drive.

The Setup Wizard should automatically run, but if not then select **Run** from the **Start** menu and type **z:\setup.exe** (where **z** is the letter of your CD drive), or use Windows Explorer to find the program.

*SnapGear Set Up Wizard* will install some files onto your PC, then attempt to find your SnapGear appliance on the network. At this point, the installation procedure diverges and a popup window will display either **A**, **B** or **C**.

**A. Your SnapGear appliance was found on the network.**

(A) Your device was found
A SnapGear device has been found at the address below.
IP address: 192.168.160.67
MAC address: 00-d0-cf-00-c5-a9
Is this the device that you wish to setup?
NOTE: the MAC address of your device can be found on the underside of the box.
Yes
No

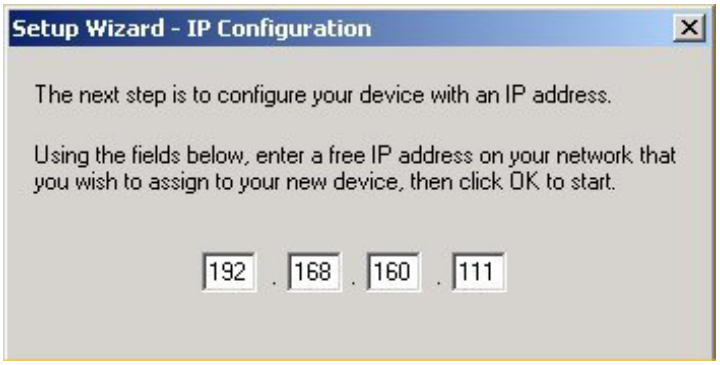
This means either your network is DHCP enabled and another PC on the network has already given it an IP address, or you have chosen to boot the SnapGear appliance with an initial, static IP address. If this is the case, skip to *Administrative Password* further on in this chapter.

**B. Multiple SnapGear appliances were found on the network.**

(B) Multiple devices found
A SnapGear device has been found at the address below.
IP address: 192.168.160.1
MAC address: 00-d0-cf-00-b1-aa
Is this the device that you wish to setup?
NOTE: the MAC address of your device can be found on the underside of the box.
Yes
No

This means your network is DHCP enabled. If this is the case, SnapGear Setup Wizard will prompt you to select which SnapGear VPN Router you wish to configure, based on its LAN port MAC address. The SnapGear Setup Wizard will display each of the different SnapGear VPN Routers that were found on the network. When the appropriate one is displayed, click "Yes" to indicate that this is the unit you want to configure. Your SnapGear VPN Router's LAN port MAC address is printed on its underside of the unit. Make the appropriate selection, then skip to *Administrative Password* further on in this chapter.

### C. Your SnapGear appliance needs an IP address.


Setup Wizard - IP Configuration
The next step is to configure your device with an IP address.
Using the fields below, enter a free IP address on your network that you wish to assign to your new device, then click OK to start.
192 . 168 . 160 . 111

This means your network is *not* DHCP enabled and you must perform the following steps:

Enter the IP address that you want to assign to your SnapGear appliance. *SnapGear Setup Wizard* will already have auto-completed the IP address. Verify that this address is acceptable and not already in use, and click OK.

*SnapGear Setup Wizard* will check that the IP address you selected isn't already in use. If it is you will be asked to make a new selection, otherwise it is assigned to your SnapGear appliance. Note that this may take a few seconds.

Your SnapGear VPN Router is now set up with an IP address so all front panel LEDs (except *System/TST/Heart Beat*) will stop flashing.

## Administrative password

After an IP address is allocated or the SnapGear appliance has been located, the SnapGear Setup Wizard will prompt you to change the SnapGear appliance administrative password. This password controls access to the *SnapGear Management Console* web administration pages.

SnapGear recommends that you select a new password that is easy for you to remember but difficult for other people to guess. Your password must be kept secret to maintain the security provided by the SnapGear appliance.

## SnapGear Management Console web administration pages

Your SnapGear appliance is now configured. The Setup Wizard will prompt you to launch a web browser to open the *SnapGear Management Console* web administration pages.

The *SnapGear Management Console* web administration pages is where you can configure the additional features of your SnapGear appliance.

To access the web administration pages, select **Management Console** under **SnapGear** in the Start menu. Alternately you can point your web browser to the SnapGear appliance's IP address (e.g. **`http://192.168.0.1`**).

If you cannot access the web administration pages, check that your browser proxy settings are correctly configured. In Microsoft's Internet Explorer, the settings are modified in *Tools*, *Internet Options*, *Connection* tab, *LAN settings*.

# SnapGear Quick Setup

After completing the initial network setup, you can use the *SnapGear Management Console* web administration pages for the common configuration tasks.

The Quick Setup Wizard will guide you through the basic steps for configuring the LAN port for your SnapGear appliance and connecting to the Internet.

To start, click the **Quick Setup Wizard** link on the *SnapGear Management Console* web administration home page. To modify the configuration, you need to enter the administrator username and SnapGear appliance administrative password. The username is **root**, the default factory password is **default**.

## LAN port quick setup

The following figure shows the LAN port quick setup:

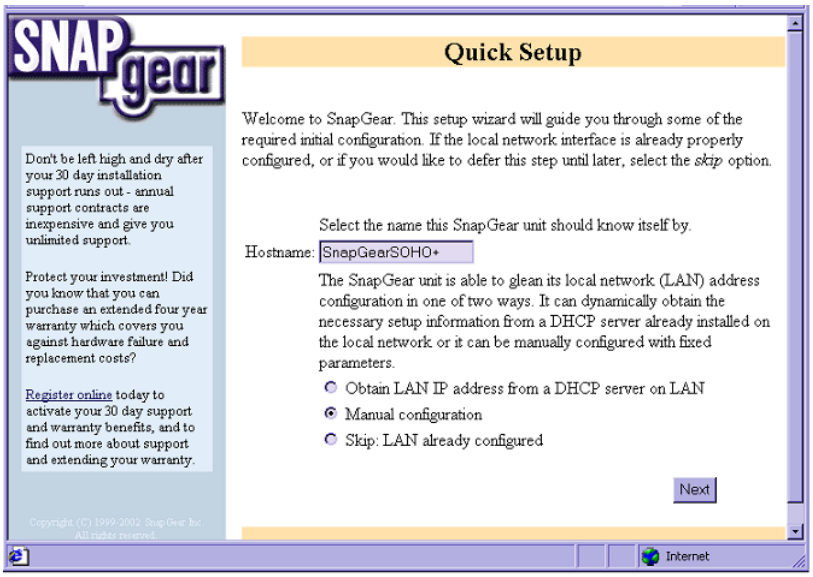

SNAP gear
Quick Setup
Welcome to SnapGear. This setup wizard will guide you through some of the required initial configuration. If the local network interface is already properly configured, or if you would like to defer this step until later, select the skip option.
Don't be left high and dry after your 30 day installation support runs out - annual support contracts are inexpensive and give you unlimited support.
Protect your investment! Did you know that you can purchase an extended four year warranty which covers you against hardware failure and replacement costs?
Register online today to activate your 30 day support and warranty benefits, and to find out more about support and extending your warranty.
Select the name this SnapGear unit should know itself by.
Hostname: SnapGearSOHO+
The SnapGear unit is able to glean its local network (LAN) address configuration in one of two ways. It can dynamically obtain the necessary setup information from a DHCP server already installed on the local network or it can be manually configured with fixed parameters.
Obtain LAN IP address from a DHCP server on LAN
Manual configuration
Skip: LAN already configured
Next
Internet

**Figure 2.3 LAN port quick setup**

1. Enter the name for your SnapGear appliance on the LAN.

2. Select the method for setting the LAN port network address configuration (either DHCP or manual).

3. If you select **DHCP** or **Skip**, the **Next** button will take you to the **ISP Connection** configuration page.

4. If you select **Manual,** the **Next** button shows the **Manual LAN Configuration** page where you must enter an **IP address** and a **Subnet mask** for the SnapGear appliance's LAN port.

## ISP connection quick setup

The following figure shows the ISP connection quick setup:

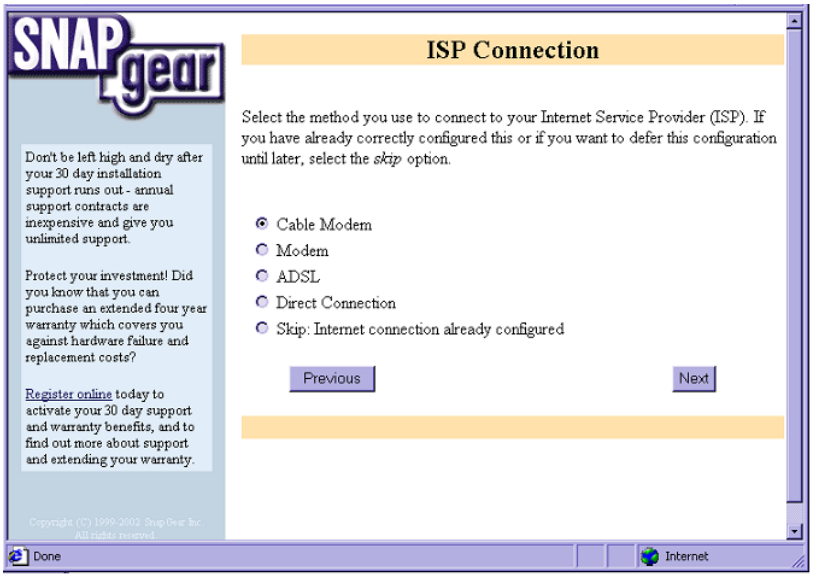

SNAPgear
ISP Connection
Select the method you use to connect to your Internet Service Provider (ISP). If you have already correctly configured this or if you want to defer this configuration until later, select the skip option.
Cable Modem
Modem
ADSL
Direct Connection
Skip: Internet connection already configured
Previous
Next
Don't be left high and dry after your 30 day installation support runs out - annual support contracts are inexpensive and give you unlimited support.
Protect your investment! Did you know that you can purchase an extended four year warranty which covers you against hardware failure and replacement costs?
Register online today to activate your 30 day support and warranty benefits, and to find out more about support and extending your warranty.
Done
Internet

**Figure 2.4 ISP connection quick setup**

Select **Cable Modem, Modem, ADSL,** or **Direct Connection** as the method for connecting to your ISP. **Direct Connection** should be used where the SnapGear appliance's Internet Port is connected to a LAN with another gateway to the Internet.

For cable modems, you need to enter your Cable Modem Service Provider. This is usually **Generic Cable Modem Provider**.

If you use an external analog modem to connect to your ISP, specify:

- The serial port connected to your modem, or that the phone line is connected directly to the PRO+'s internal modem.
- The name of your ISP.
- The phone number used to dial your ISP. If your ISP has provided you with multiple phone numbers, you may enter them separated with commas. If you wish to incorporate a comma into the dial string, prefix it with a backslash, i.e.: `\,`
- The username and password for your ISP account.

- The DNS server for your ISP (optional). Multiple DNS addresses may be entered separated by commas. Note that any DNS addresses automatically handed out by your ISP will take precedence over the addresses specified here.

If you use ADSL (Asymmetric Digital Subscriber Line) to connect to your ISP, you must specify the ADSL connection type. This can be done in one of the following ways:

- **Auto Detect.** Allow your SnapGear appliance to automatically detect your ADSL connection type. *This is the best choice in most cases.*

- **Use PPPoE to connect.** Select this option if your ADSL modem communicates using PPPoE, i.e. your ISP has given you a username and password to authenticate your DSL connection. You will also be asked to specify:

    - The username and password for your ADSL connection.

    - If you want to **connect on demand** or stay connected continuously (the best choice in most cases).

    - For **connect on demand** connections, you need to specify the **idle disconnect time** (in minutes).

- **Use DHCP to connect.** DHCP is used if your ISP requires you to get an IP address automatically from a DHCP server over the Internet.

- **Manually assign settings.** Select this option if your ISP provides a fixed IP address and a subnet mask and (optionally) a gateway address and a DNS address to be configured into the computer connecting to the ADSL modem.

- For a **Direct Connection** you must configure the Internet port to either get its address information via DHCP or manually enter static values for **IP Address, Subnet Mask, Gateway Address,** and **DNS Address.** The **Gateway Address** is the address of the host where all Internet network traffic is initially directed for further processing. The **DNS Address** is the address of the host that translates Internet domain names into IP addresses. Multiple DNS addresses may be entered separated by commas.

# Setup PCs to access the Internet

To access the Internet, the PCs on your network must all be set up to use the SnapGear appliance as the default gateway. This can be done a number of different ways depending on how your network is set up.

If your network is already DHCP enabled, proceed to *DHCP enabled network*.

If your network is NOT DHCP enabled, proceed to *Non DHCP enabled network*.

If you are not sure then you probably want *Non DHCP enabled network*.

## DHCP enabled network

Add a lease to your existing DHCP server to exclude the IP address that was assigned to your SnapGear appliance.

Enter this same IP address as the gateway IP address to be given out by the DHCP server.

By default, your SnapGear appliance acts as a DNS proxy. If you have not changed this option, enter the SnapGear appliance's LAN IP address as the DNS IP address to be given out by the DHCP server. If you have disabled the DNS proxy on the SnapGear appliance, enter the DNS IP address given by your Internet Service Provider instead.

Restart all the PCs on the network (this will reset their gateway and DNS addresses).

***Note***

*The purpose of restarting the computers is to force them to gain a new DHCP lease. Alternatively you can use utilities such as winipcfg (Windows 95/98/Me) or ipconfig (Windows 2000/XP), to release then renew a lease.*

## Non DHCP enabled network

A DHCP enabled network allows PCs to automatically get network set up information when they start up. If your network is not DHCP enabled, you may either manually set up each PC on your network, or choose to enable DHCP on your network by activating the SnapGear appliance's inbuilt DHCP server.

***Note***

*If you only have a single PC we suggest manually setting up your network, but if you intend to have more computers then enabling the SnapGear appliance's DHCP server is more scalable.*

***Note***

*If you need to manually set up IP addresses we suggest a private range of 192.168.0.1 (subnet mask 255.255.255.0) for your computers, and setting your SnapGear appliance to be 192.168.0.254. This is preferable to relying on Windows "auto IP" address assignment.*

To manually set up each Windows PC on your network (example given is for Windows 95/98/Me and is similar to Windows 2000 and others):

Click **Start**, choose **Settings**, then **Control Panel**, then double click **Network** and in the **Configuration** pane (**Protocols** in NT, right click on the connection and choose **Properties** in 2000 and XP), select **TCP/IP** (**TCP/IP ->** *[your network card name]* if there are multiple entries).

Click **Properties**.

Click **Gateway** and enter the IP address that you assigned to your SnapGear appliance. Click **Add**, then click **OK**

Click **DNS Configuration** and enter:

- The SnapGear appliance's LAN IP address if the SnapGear appliance is acting as a DNS proxy (this is the default)

*OR*

- The DNS address that was given to you by your Internet Service Provider, if the SnapGear appliance is not acting as a DNS proxy.

Click **Add**, then **OK**. Reboot the PC if prompted to do so.

Perform these steps for each PC on your network.

You are now finished.

Alternatively, to activate your SnapGear appliance's DHCP server:

Click **Start**, choose **Programs**, then **SnapGear** and click **SnapGear Management Console**. This will take you to the *SnapGear Management Console* web administration pages.

Select **DHCP Server** from the **Network** menu

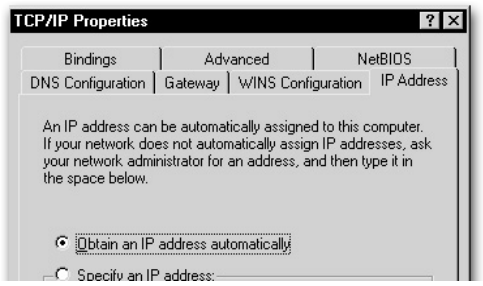
Click **Configure** in the **DHCP Server Settings** section to configure the DHCP server's **Gateway Address**, **DNS Address**, **WINS Address**, and **Lease Times**. Check **Enable DHCP Server** and click **Apply**. For a detailed description of configuring DHCP Server Settings, please refer to the *DHCP server* section in Chapter 6.

Enter the range of IP addresses you wish to have the SnapGear appliance assign to PCs on your network by clicking **Configure** in the **Dynamic Addresses** section. Then follow the instructions in the **Add/Remove Addresses** section of the **DHCP Dynamic Address Configuration** page.

Your network is now DHCP enabled. Each PC on the network must now be set up to use DHCP.

For each PC on the network, click **Start**, choose **Settings**, then **Control Panel**, then double click **Network** and in the **Configuration** pane (**Protocols** in NT, right click on the connection and choose **Properties** in 2000 and XP), select **TCP/IP** (**TCP/IP -> *[your network card name]*** if there are multiple entries).

Click **Properties**, click the **IP Address** tab and check **Obtain an IP address automatically** and click **OK**. Reboot the PC if prompted to do so.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:

To access the Internet, all PCs on your network must have:

- The IP address of the SnapGear appliance defined as their default gateway, and
- The DNS server provided by the ISP, or the SnapGear appliance's DNS proxy.

You can enter these details manually (i.e. statically), or they can be dynamically assigned by a DHCP server each time the PC boots.

To take advantage of the SnapGear appliance's DHCP server (or if you are already using a DHCP server on the network), configure the computers on your network to use DHCP.

If you are using Windows 95/98, click the **Configuration** panel, **TCP/IP ->** *[your network card name]*, **Properties**, then the **IP Address** panel.

If you are using Windows NT 4, click the **Protocols** panel, **TCP/IP**, **Properties**, and then the **IP Address** panel.

If you are using Windows 2000, click **Start**, **Settings**, **Network and Dial-up Connections**, right-click **Local Area Connection**, click **Properties**, select **Internet Protocol** and then click **Properties** to display the following screen:

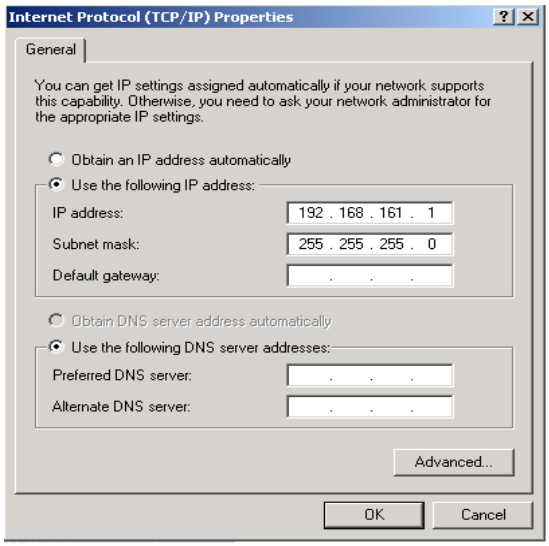

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 161 . 1
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

**Figure 2.3 TCP/IP properties**

You can also manually configure the PCs on your network. For each non-configured Windows 2000 PC on the network, open **TCP/IP Properties** using the above instructions and ensure that **Use the following IP address** is checked and add the following information:

- A unique IP address and appropriate subnet mask.
- The Default Gateway (enter the IP address of the SnapGear appliance).
- In the **DNS** tab, enter the DNS server address(es) provided by your ISP, or the address of the SnapGear appliance if you are using the DNS proxy.

# SnapGear PCI appliances

This section walks you through the installation of your SnapGear appliance. Installing your SnapGear appliance into a well-planned network is quick and easy. However, network planning and design is outside the scope of this guide. Please take some time to plan your network prior to installing your SnapGear appliance.

These steps presume that you already have a PC running Windows 2000 or Windows XP.

***Note***

*It is possible to install a SnapGear appliance into PCs running other operating systems by installing a Realtek RTL8139-series Fast Ethernet Adapter driver as you would for a regular NIC.*

Power off your PC and remove its cover.

Select an unused PCI slot and insert the SnapGear appliance.

Connect the SnapGear appliance's network port to the LAN using an Ethernet cable.

Power on your PC.

***Note***

*The rear panel LEDs provide information on the operating status of your SnapGear appliance. The two LEDs closest to the network port indicate network link and activity.*

*The two LEDs furthest from the network port indicate Power and Heartbeat. The Heartbeat LED blinks when the SnapGear appliance is running. The Power LED is ON when power is applied and the SnapGear has acquired an IP address. Initially, both of these LEDs will be blinking.*

*If the Power and Heartbeat LEDs do not blink then try pressing the Reset button on the rear panel before attaching the appliance to the network. If after doing this these LEDs are not blinking, you may need to contact customer support.*

The SnapGear appliance will be automatically detected and have the appropriate driver installed when Windows starts up. It will be detected as a Realtek RTL8139-series Fast Ethernet Adapter.

***Note***

*You can check that a new network adapter has been installed by clicking **Start**, **Settings**, **Network and Dialup Connections**, **Local Area Connection** (possibly followed by a number), **Properties** and ensure the adapter is listed in **Connect** using field.*

To communicate on your network, your SnapGear appliance will need to be configured with two IP addresses. One is used to manage the SnapGear appliance. The other is the host PC's IP address – this is the IP address that other PCs on the LAN see.

At this point, the installation procedure diverges depending on whether your network has an existing DHCP server.

**Check the rear panel of the SnapGear appliance. If the Heartbeat LED is flashing and the Power LED is on, proceed to A. If both the Heartbeat and Power LEDs are flashing, proceed to B**.

**A. An existing DHCP server has assigned IP addresses to your SnapGear appliance.**

Assuming your existing network is appropriately configured, you should now be able to access the Internet.

Insert the SnapGear Installation CD into your CD drive to install supporting software and documentation for your SnapGear appliance.

The Setup Wizard should automatically run, if not select **Run** from the Start menu and type **z:\setup.exe** (where *z* is the letter of your CD drive), or use Windows Explorer to find the program.

(A) Your device was found
A SnapGear device has been found at the address below.
IP address: 192.168.160.67
MAC address: 00-d0-cf-00-c5-a9
Is this the device that you wish to setup?
NOTE: the MAC address of your device can be found on the underside of the box.
Yes
No

SnapGear Setup Wizard will install some files onto your PC, then locate your SnapGear appliance on the network. If multiple SnapGear appliances are located, SnapGear Setup Wizard will prompt you to select which SnapGear appliance you wish to configure based on its MAC address. The MAC address is located on the SnapGear appliance's box.

**B. Your SnapGear appliance requires IP addresses.**

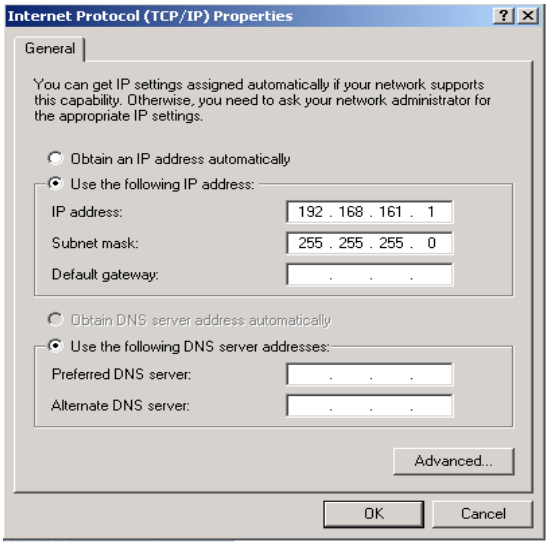
First, set the host PC's IP address through Windows Settings.

Click **Start**, **Settings**, **Network and Dialup Connections**, **Local Area Connection** (possibly followed by a number) then **Properties**.

Ensure the TCP/IP protocol is installed. If not, Click **Install**, **Protocol**, **Add**, then **Internet Protocol (TCP/IP)**.

Highlight **TCP/IP** and click **Properties**.

In the **IP Address** panel, select **Use the following IP address**.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 161 . 1
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

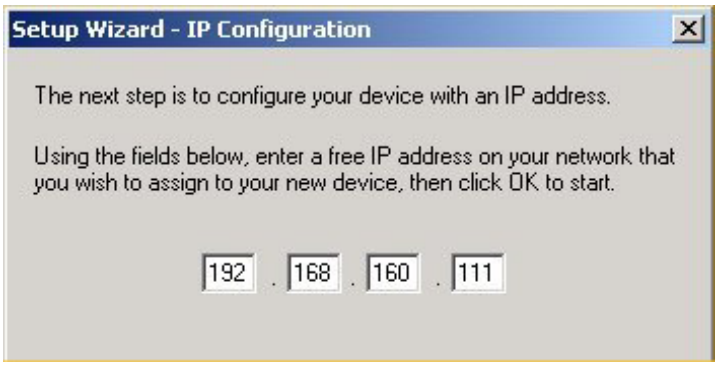
If the **IP Address** field, enter a free IP address in the same range as the rest of your LAN. Enter **subnet mask**, **default gateway** and **DNS server** information that reflects your LAN configuration.

Insert the SnapGear Installation CD into your CD drive to install supporting software and documentation for you SnapGear appliance, and assign it an IP address.

The Setup Wizard should automatically run, if not select **Run** from the Start menu and type **z:\setup.exe** (where *z* is the letter of your CD drive), or use Windows Explorer to find the program.

***Note***

*It is recommended at this point that you detach the network cable from the SnapGear appliance network port.*


Setup Wizard - IP Configuration
The next step is to configure your device with an IP address.
Using the fields below, enter a free IP address on your network that you wish to assign to your new device, then click OK to start.
192 . 168 . 160 . 111

SnapGear Setup Wizard will install some files onto your PC, then prompt you to enter a free IP address to assign your SnapGear appliance. This must be different from the address you have just assigned through Windows Settings, but in the same range.

## Administrative password

After an IP address is allocated or the SnapGear appliance has been located, the SnapGear Setup Wizard will prompt you to change the SnapGear appliance administrative password. This password controls access to the *SnapGear Management Console* web administration pages.

SnapGear recommends that you select a new password that is easy for you to remember but difficult for other people to guess. Your password must be kept secret to maintain the security provided by the SnapGear appliance.

## SnapGear Management Console web administration pages

Your SnapGear appliance is now configured. The Setup Wizard will prompt you to launch a web browser to open the *SnapGear Management Console* web administration pages.

The *SnapGear Management Console* web administration pages is where you can configure the additional features of your SnapGear appliance.

To access the web administration pages, select **Management Console** under **SnapGear** in the Start menu. Alternately you can point your web browser to the SnapGear appliance's IP address (e.g. **`http://192.168.0.1`**).

If you cannot access the web administration pages, check that your browser proxy settings are correctly configured. In Microsoft's Internet Explorer, the settings are modified in *Tools*, *Internet Options*, *Connection* tab, *LAN settings*.

## Disabling the Reset button

For convenience, the SnapGear appliance ships with the rear panel Reset button enabled. This allows the SnapGear appliance's configuration to be reset to factory defaults. From a network security standpoint, it may be desirable to disable the Reset switch after initial setup has been performed. This can accomplished by removing the jumper linking *CON2* on the SnapGear appliance.

# 3. Connecting to the Internet

This chapter provides step-by-step instructions for connecting your SnapGear appliance to your Internet Service Provider (ISP).

The SnapGear appliance provides secure Internet access using its robust embedded firewall. The SnapGear appliance has an IP masquerading feature, which means that users on your local network can see the outside world; however the outside world cannot see inside your local network. This shields your network from intruders and also allows you to filter packets (see Chapter 7*, Firewall*) to prevent unwanted traffic to/from your network.

The SnapGear appliance can connect to the Internet using an external dialup analog modem, an ISDN modem, a permanent analog modem, a cable modem or DSL link as shown in the following figure:

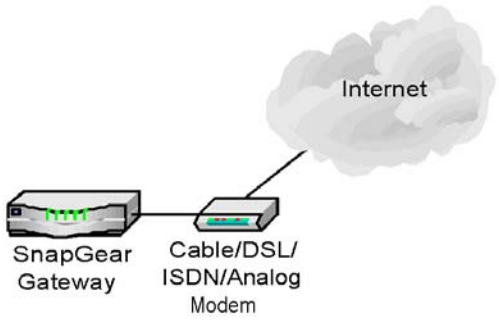



**Figure 3.1 Internet connection**

## Physically connect modem device

The first step in connecting your office network to the Internet is to physically attach your SnapGear appliance to the modem device. For analog modems, attach the modem serial cable to the SnapGear appliance's serial port (i.e. *COM1* or *COM2*). The SnapGear PRO+ has an integrated internal analog modem that you may use instead of attaching an external analog modem. For cable and DSL connections plug the Ethernet cable from the modem into the *Internet* port.

***Warning***

*To connect to an ISDN line, the SnapGear appliance requires an intermediate device called a Terminal Adapter (TA). A TA connects into your ISDN line and has either a serial or Ethernet interface that is connected to your SnapGear appliance. Do NOT plug an ISDN connection directly in to your SnapGear appliance.*

# Select Internet connection

***Note***

*SME570 and SME575 use a different interface for configuring its network interfaces. See Chapter 4, Network Setup and DMZ.*

The next step is to select the method for connecting your SnapGear appliance to the Internet. From the *SnapGear Management Console* web administration pages**,** in the **Networking** menu, select **Connect to Internet** and select the method to connect to your local ISP. You can connect using a cable, ISDN, DSL or analog modem connection. Select the connection type and click **Continue**.

## Connect to Internet – cable modem

If you are connecting to the Internet using a cable modem, select a **Cable** connection, select your cable ISP from the list and click **Next**. If your provider does not appear, select *Generic Cable Modem Provider.* For cable modem providers other than Generic, enter your username and password and click **Finish**. You are now ready to connect. Click the **Reboot** button to save your configuration and reboot your SnapGear appliance.

## Connect to Internet – ADSL

If you are connecting to the Internet using ADSL, you must select the connection method **PPPoE, DHCP,** or **Manually Assign Settings.** Alternatively, the SnapGear appliance can determine the connection method automatically (recommended).

Use PPPoE if your ISP uses username and password authentication to access the Internet. Use DHCP if your ISP does not require a username and password, or if your ISP instructed you to obtain an IP address dynamically. If your ISP has given you an IP address or address range, you must manually assign the settings on the SnapGear appliance's Internet interface. Select the appropriate method and click **Apply.**

For PPPoE, enter the username and password for your ISP account. By default, your SnapGear appliance maintains the ADSL connection continuously; however you can change this if required to **Connect on Demand**. For on demand connections, enter an **Idle Disconnect Time**. This is the time (in minutes) that the SnapGear appliance will wait before disconnecting if the line is idle.

DHCP connections may also require a host name for your SnapGear appliance. Select **Manually Assign Settings** and enter the **IP Address** and **Netmask** and optionally the **Gateway** and the **DNS Address** if provided by your ISP. Multiple DNS addresses may be entered separated by commas. Note that any DNS addresses automatically handed out by your ISP will take precedence over these addresses. Reboot the SnapGear appliance for the new configuration to take effect.

If you are unsure of the **ADSL Connection Method**, select **Auto detect ADSL connection type** and your SnapGear appliance will attempt to automatically determine the connection method.

## Connect to Internet – direct

Choosing **Direct Connection** to the Internet shows the **IP Configuration** page. See the section called IP Configuration in Chapter 6, *Network Configuration.*

## Connect to Internet – modem

The following figure shows the Setup modem Internet connection:

**Figure 3.2 Setup modem Internet connection**

If you are connecting to the Internet using a modem, the system displays the **Connect to Internet via a Modem** screen. The following table describes the fields and explains how to configure the dial up connection to your ISP.

| Field | Description |
|---|---|
| Serial port to dial-out on | Select the SnapGear appliance COM (serial) port you will use for the modem that will dial your ISP. On the SnapGear PRO+ you may also select *Modem* to use the internal modem. This port will be dedicated for the Internet connection; any attempt to dial-in using this COM port will be blocked.<br>Note: If a port was previously setup for dial-in and is later enabled for Internet access, the dial-in function is automatically disabled. |
| Name of Internet provider | Enter the name of your ISP. |
| Phone number(s) to dial | Enter the number to dial to reach your ISP. If you are behind a PABX that requires you to dial a prefix for an outside line (e.g. 0 or 9) ensure you enter the appropriate prefix. If your ISP has provided you with multiple phone numbers, you may enter them separated with commas. |
| ISP DNS Server(s) (*optional*) | Enter the DNS server address supplied by your ISP. Multiple DNS addresses may be entered separated by commas. Note that any DNS addresses automatically handed out by your ISP will take precedence over the addresses specified here. |
| Username and password | Enter the unique username and password allocated by your ISP. The **Password** and **Confirm Password** fields must match. |

Click **Advanced** to configure the following options.

| Field | Description |
|---|---|
| Idle timeout | By default, the SnapGear appliance dials-on-demand (i.e. when there is traffic trying to reach the Internet) and disconnects if the connection is inactive (i.e. when there is no traffic to/from the Internet) for 15 minutes. If using dial-on-demand, this value can be set from 0 to 99 minutes.<br>Selecting **Stay Connected** will disable the idle timeout. |
| Redial setup | If the dial up connection to the Internet fails, **Max Connection Attempts** specifies the number of redial attempts to make before discontinuing . **Time Between Redials** specifies the number of seconds to wait between redial attempts. |
| Statically assigned IP address | The majority of ISPs dynamically assign an IP address to your connection when you dial-in. However some ISPs use pre-assigned static addresses. If your ISP has given you a static IP address, enter it in **Local IP Address** and enter the address of the ISP gateway in **Remote IP Address**. |

Once the connection has been setup, **Connect**/**Disconnect** buttons will be displayed. These make the SnapGear appliance dial or hang up the modem connection immediately.

## Internet failover

SnapGear appliances are designed with the real Internet in mind, which may mean downtime due to ISP equipment or telecommunications network failure. Failures can be caused by removing the wrong plug from the wall, typing in the wrong ISP password or many other reasons. Regardless of the cause of a failure it can potentially be very expensive.

Failover provides the ability to use a low-speed connection when the high-speed connection fails to allow services to continue operating. When the main Internet connection fails and the backup connection (or failover) is started, VPN connections are restarted and dynamic DNS services are advised of the new IP address.

After configuring a normal Internet connection, a link to the Internet failover page allows you to configure failover support. You can also access the failover page by clicking **Connect To Internet** in the **Networking** menu.

The following figure shows the advanced configuration options:

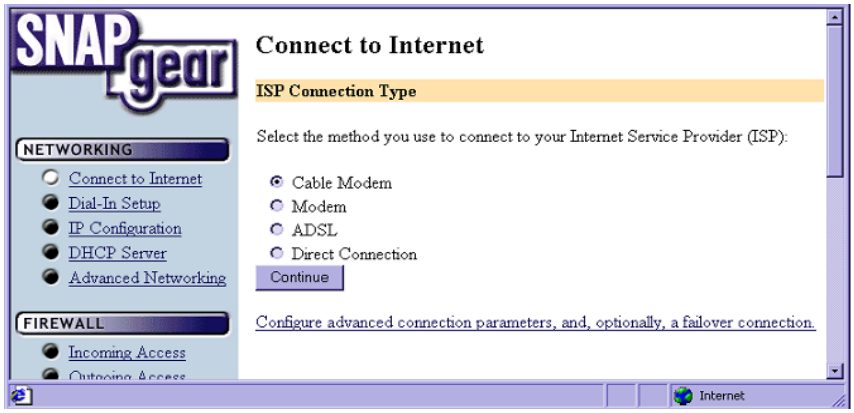



**Figure 3.3 Advanced configuration option**

The following figure shows the failover configuration screen:

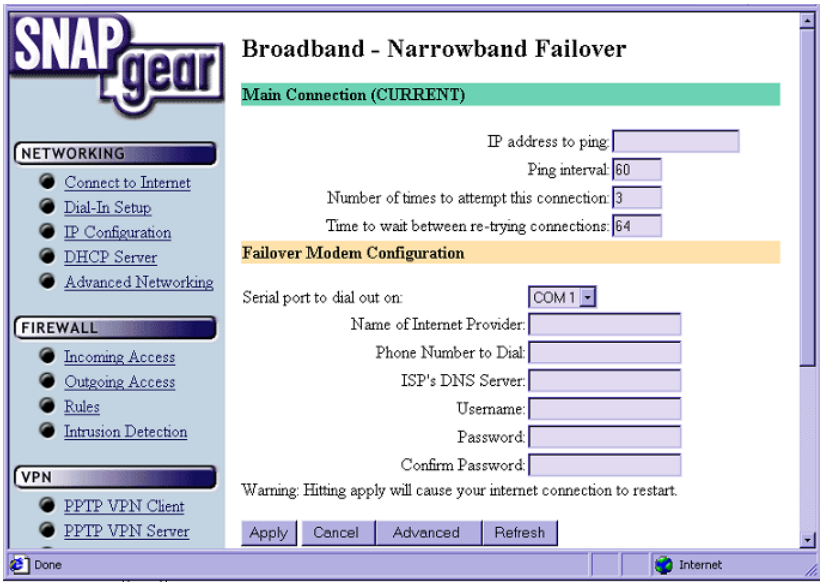



**Figure 3.4 Failover configuration screen**

The following fields can be configured for the failover connection.

| Field | Description |
|---|---|
| IP Address to ping | IP address the SnapGear appliance will ping to determine if the Internet connection is up or down. |
| Ping Interval | How often to ping the remote machine to determine if the Internet connection is up or down. |
| Number of times to attempt this connection | Number of times to attempt the connection before the SnapGear appliance moves to the failover connection. |
| Time to wait between re-trying connections | The Internet connection fails immediately when the password is wrong, or if the SnapGear appliance is unable to contact an ADSL modem to make a connection. Specify the time to wait between retrying this connection after detecting the initial failure. |
| Fall forward *(only available after configuring the failover connection)* | Allow the SnapGear appliance to continue trying the main Internet connection until the connection is established. At this point the SnapGear appliance disconnects the backup Internet connection and continues using the main Internet connection. |
| Enable failover *(only available after configuring the failover connection)* | Checking this box indicates you want the SnapGear appliance to use the backup Internet connection if the SnapGear appliance detects that the main Internet connection has failed. |

## Failed connection

An Internet connection is considered failed if the SnapGear appliance tests the Internet connection the specified number of times, and fails each time. The SnapGear appliance can test the Internet connection by ensuring that the physical connection was made correctly (i.e. an IP address was received from the ISP), and then pinging a remote host.

For some Internet connections (e.g. PPPoE ADSL) you may need to ping a remote host to determine if the Internet connection is up or down. The SnapGear appliance will usually detect if a PPPoE ADSL Internet connection is down.

For Internet connection types that require you to specify a static IP address or use DHCP, the SnapGear appliance cannot usually detect if the Internet connection is down. To ensure that the Internet connection is up, enter a host for the SnapGear appliance to ping.

If the Internet connection fails, the SnapGear appliance will attempt to reconnect to the Internet using the main connection for the number of specified times. After each failed attempt, the SnapGear appliance will wait the number of seconds specified.

For PPPoE and dial-up connections, the SnapGear appliance sends an echo request (ping) and the remote machine responds with an echo reply. The main connection is considered down if more than three echo replies do not appear.

***Warning***

*You currently cannot failover for an ADSL demand dial-internet connection, or for any type of analog modem connection.*

# Configure PCs to use SnapGear appliance Internet gateway

The PCs on your network must be configured to use the SnapGear appliance as the default gateway for Internet access. See the section called *Setup PCs to access the Internet*.

To access the Internet, the PCs on your network must all be set up to use the SnapGear appliance as the default gateway. This can be done a number of different ways depending on how your network is set up.

**If your network is already DHCP enabled, proceed to *DHCP enabled network*.**

**If your network is NOT DHCP enabled, *Non DHCP enabled network*.**

**If you are not sure then you probably want *Non DHCP enabled network*.**

## DHCP enabled network

Add a lease to your existing DHCP server to exclude the IP address that was assigned to your SnapGear appliance.

Enter this same IP address as the gateway IP address to be given out by the DHCP server.

By default, your SnapGear appliance acts as a DNS proxy. If you have not changed this option, enter the SnapGear appliance's LAN IP address as the DNS IP address to be given out by the DHCP server. If you have disabled the DNS proxy on the SnapGear appliance, enter the DNS IP address given by your Internet Service Provider instead.

Restart all the PCs on the network (this will reset their gateway and DNS addresses).

***Note***

*The purpose of restarting the computers is to force them to gain a new DHCP lease. Alternatively you can use utilities such as winipcfg (Windows 95/98/Me) or ipconfig (Windows 2000/XP), to release then renew a lease.*

## Non DHCP enabled network

A DHCP enabled network allows PCs to automatically get network set up information when they start up. If your network is not DHCP enabled, you may either manually set up each PC on your network, or choose to enable DHCP on your network by activating the SnapGear appliance's inbuilt DHCP server.

***Note***

*If you only have a single PC we suggest manually setting up your network, but if you intend to have more computers then enabling the SnapGear appliance's DHCP server is more scalable.*

***Note***

*If you need to manually set up IP addresses we suggest a private range of 192.168.0.1 (subnet mask 255.255.255.0) for your computers, and setting your SnapGear appliance to be 192.168.0.254 This is preferable to relying on Windows "auto IP" address assignment.*

To manually set up each Windows PC on your network (example given is for Windows 95/98/Me and is similar to Windows 2000 and others):

Click **Start**, choose **Settings**, then **Control Panel**, then double click **Network** and in the **Configuration** pane (**Protocols** in NT, right click on the connection and choose **Properties** in 2000 and XP), select **TCP/IP** (**TCP/IP *-> [your network card name]*** if there are multiple entries).

Click **Properties**.

Click **Gateway** and enter the IP address that you assigned to your SnapGear appliance. Click **Add**, then click **OK**

Click **DNS Configuration** and enter:

The SnapGear appliance's LAN IP address if the SnapGear appliance is acting as a DNS proxy (this is the default)

OR

The DNS address that was given to you by your Internet Service Provider, if the SnapGear appliance is not acting as a DNS proxy.

Click **Add**, then **OK**. Reboot the PC if prompted to do so.

Perform these steps for each PC on your network.

You are now finished.

Alternatively, to activate your SnapGear appliance's DHCP server:

Click **Start, Programs**, then **SnapGear** and click **SnapGear Management Console**. This will take you to the SnapGear Management Console web administration pages.

Select **DHCP Server** from the **Network** menu

Click **Configure** in the **DHCP Server Settings** section to configure the DHCP server's **Gateway Address**, **DNS Address**, **WINS Address**, and **Lease Times**. Check **Enable DHCP Server** and click **Apply**. For a detailed description of configuring DHCP Server Settings, please refer to the *DHCP server* section in Chapter 6.

Enter the range of IP addresses you wish to have the SnapGear appliance assign to PCs on your network by clicking **Configure** in the **Dynamic Addresses** section. Then follow the instructions in the **Add/Remove Addresses** section of the **DHCP Dynamic Address Configuration** page.

Your network is now DHCP enabled. Each PC on the network must now be set up to use DHCP.

For each PC on the network, click **Start**, choose **Settings**, then **Control Panel**, then double click **Network** and in the **Configuration** pane (**Protocols** in NT, right click on the connection and choose **Properties** in 2000 and XP), select **TCP/IP** (**TCP/IP -> *[your network card name]*** if there are multiple entries).

Click **Properties**, click the **IP Address** tab and check **Obtain an IP address automatically** and click **OK**.  Reboot the PC if prompted to do so.

## Establishing the connection

If you are connecting to your ISP using a modem, the **Connect**/**Disconnect** buttons make the SnapGear appliance dial or hang up the modem connection immediately.

If you are connecting to your ISP using a modem or ISDN connection, the SnapGear appliance will automatically place a call when an application requires access to the Internet (e.g. sending e-mail, browsing the web, etc).

To establish the connection:

1. From any PC on the network, launch a browser application (e.g. Internet Explorer or Netscape Navigator).

2. The SnapGear appliance will dial the ISP and log in. On the front panel, the *COM*/*Serial Activity*/*TX/RX* LED will flash when establishing the connection.

3. The *Online* LED will light when the Internet link is created and your browser will display the default home page.

4. If *Dial-on-demand/Idle time* is enabled, the SnapGear appliance will also disconnect from the Internet when the connection is idle for the specified period.

Internet access is automatic if you are using a permanent connection device (e.g. cable modem) or if you are using ADSL or an analog modem configured to stay connected.

# 4. Network Setup and DMZ

***Note***

*This chapter is specific to the SnapGear SME570 and SME575.*

This chapter describes the **Network Setup** section of the *SnapGear Management Console*. Here you can configure each of your SnapGear appliance's network interfaces (Ethernet, serial). Network interfaces may be configured for Internet connection, LAN connection, DMZ connection, remote dial-in access or Internet failover.

Configuration options accessed through the **Connect to Internet**, **Dial In Setup**, **IP Configuration** and **Advanced Networking** sections of other models have been integrated into the **Network Setup** section on the SME570 and SME575.

## Connections

Under the **Connections** tab, each of the network interfaces of your SnapGear appliance is displayed alongside its **Device Name** and current **Configuration**. Initially, all network interfaces will be unconfigured, aside from **LAN**.

A network interface can be configured for a different function by selecting a new configuration from the **Configuration** drop down box. The current configuration can be viewed or modified by selecting **Edit current settings**. Selecting **Remove this configuration** unconfigures a network interface (you will be prompted to confirm this action).

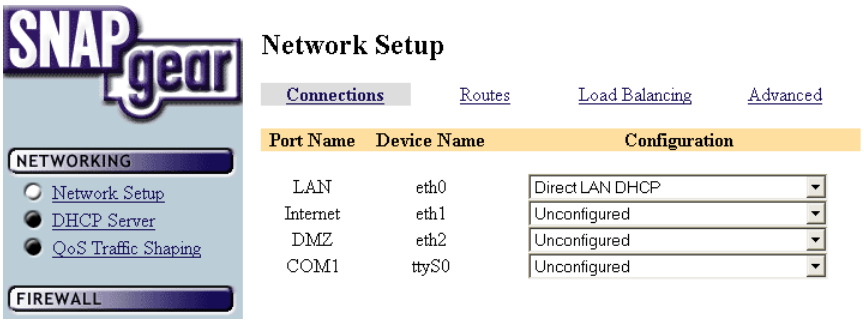



**Figure 4.1 Network Setup Connections**

Each of the network interfaces that may be present on your SnapGear appliance and how they may be configured are discussed below.

## LAN

Unlike **Internet**, **DMZ** or **COM1** interfaces, the **LAN** network interface has only one configurable function, to connect to your local area network. Network settings for the **LAN** network interface may be assigned statically, or dynamically by a DHCP server (factory default). Select **Edit current settings** to continue.

To assign network settings statically, enter an **IP Address** and **Netmask** for the **LAN** network interface. If you are using the SnapGear appliance in its default, network address translation mode, (see *Network address translation* in the *Advanced IP configuration* section of Chapter 6, *Networking Configuration*), this will typically be part of a private IP range, such as *192.168.0.1* / *255.255.255.0*. Ensure **DHCP assigned** is unchecked.

If you wish to have your SnapGear appliance obtain its LAN network settings from an active DHCP server on your local network, check **DHCP assigned** then **Apply**. Note that anything in the **IP Address** and **Netmask** fields will be ignored.

At this time you may also enter one or more **DNS servers**. Multiple servers may be entered separated by commas.

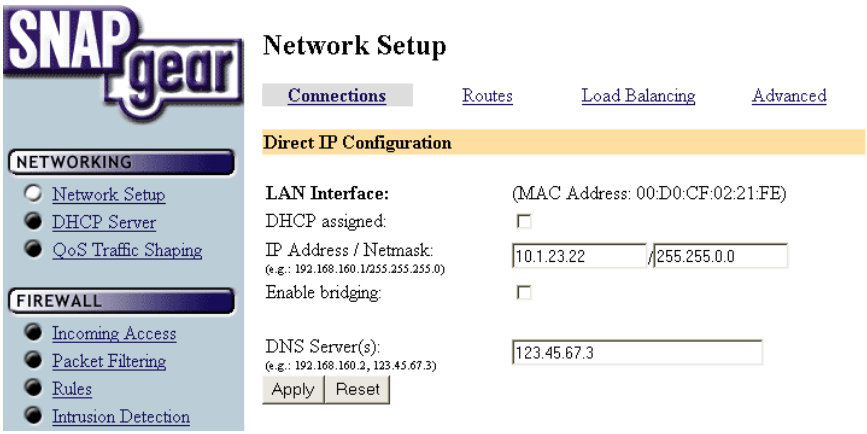



**Figure 4.2 LAN Configuration**

You may also enable bridging. This is discussed in *Bridging* in the *IP Configuration* section of Chapter 6, *Network Configuration*.

### Internet

Select the connection method you use to connect to the Internet. Refer to *Select Internet connection* onwards in Chapter 3, *Connecting to the Internet* for details on configuration options specific to your Internet connection method.

### DMZ

The **DMZ** interface on your SnapGear appliance can be configured as a DMZ connection or an Internet connection. The configuration you select affects the default behaviour of the firewall for the DMZ interface (see *Packet Filtering* in Chapter 7, *Firewall*).

- Select **Direct DMZ** if you wish to establish a physically separate DMZ network. A DMZ is used to provide better security for your LAN. If you place a publicly accessible server on your LAN, and an attacker compromises the server, then the attacker will immediately have direct access to your LAN. However, if you place the server on a physically separate network (i.e. the DMZ), and an attacker compromises the server, then the attacker will only be able to access other machines on the DMZ. The SnapGear appliance will protect machines on the LAN from the compromised server on the DMZ.

  Refer to *DMZ Configuration* later in this chapter for further details on this configuration.

- Configure the **DMZ** interface as a second Internet connection if you wish to take advantage of the load balancing capabilities of your SnapGear appliance. This is done similarly to your primary Internet connection, as described above.

  Refer to the *Load Balancing* section later in this chapter for further details on how to configure your SnapGear appliance to perform load balancing between the two connections.

### COM1

With a modem attached, the COM1 interface can be configured as a primary **Dialout Internet** connection, to provide **Dialin Access** for remote users, or as a secondary **Failover Dialout Internet** connection that will be activated should your primary Internet connection go down.

- Select **Dialout Internet** to use this interface as your primary Internet connection. Refer to *Connect to Internet – modem* in Chapter 3, *Connecting to the Internet* for further details on configuring the connection.

- Select **Dialin Internet** to use this interface as a dialin server to allow remote users to connect to your local network. Refer to Chapter 5, *Dialin Server Configuration* for further details.

- Select **Failover Dialout Internet** to use this interface as a backup dialout Internet connection, to be activated should your primary Internet connection go down. Note that this option will only become available once a primary Internet connection has been configured. Refer to the *Internet failover* section in Chapter 3, *Connecting to the Internet* for further details on configuring the failover connection.

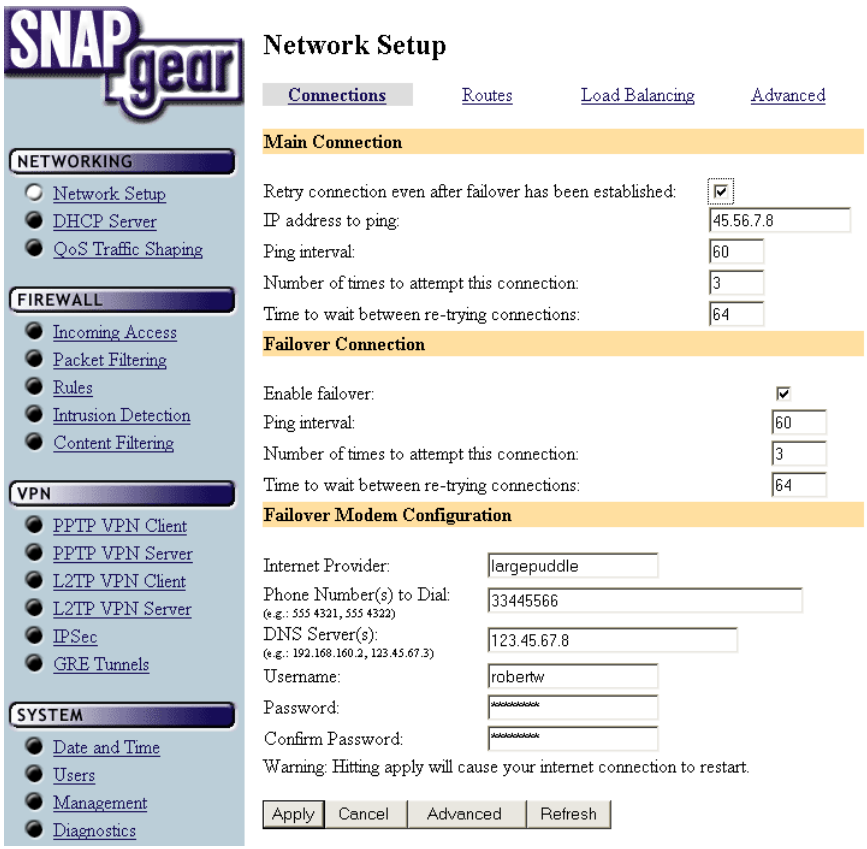



**Figure 4.3 Failover Configuration**

# DMZ Configuration

As with the **LAN** network interface, the **DMZ** interface network settings may be assigned statically, or dynamically by a DHCP server.

To assign network settings statically, enter an **IP Address** and **Netmask** for the **LAN** network interface. The DMZ network may use either a private IP address range (e.g. *10.10.0.1* / *255.255.0.0*) or real world addresses. Ensure **DHCP assigned** is unchecked.

If wish to have your SnapGear appliance obtain its LAN network settings from an active DHCP server on your DMZ network, check **DHCP assigned** then **Apply**. Note that anything in the **IP Address** and **Netmask** fields will be ignored.

### Services on the DMZ network

Once you have configured the DMZ connection, you will also want to configure the SnapGear appliance to allow access to services on the DMZ. There are two methods of allowing access.

If the servers on the DMZ have public IP addresses, you need to add packet filtering rules to allow access to the services. See the section called *Packet Filtering* in Chapter 7, *Firewall*.

If the servers on the DMZ servers have private IP addresses, you need to port forward the services. See the section called *Incoming Access* in Chapter 7, *Firewall*. Creating port forwarding rules automatically creates associated packet filtering rules to allow access. However, you can also create custom packet filtering rules if you wish to restrict access to the services.

You may also want to configure your SnapGear appliance to allow access from servers on your DMZ to servers on your LAN. By default, all network traffic from the DMZ to the LAN is dropped. See the section called *Packet Filtering* in Chapter 7, *Firewall*.

## Load balancing

If you have enabled both the **Internet** and **DMZ** network interfaces as Internet connections, you may enable Load Balancing. This will share Internet traffic load over the two connections.

To enable load balancing, check **Enable Loading Balancing** and click **Apply**.

## Routes

Refer to *Additional Routes* and *Route Management* in the *Advanced Networking* section of Chapter 6, *Network Configuration*.

## Advanced

Refer to *Advanced IP configuration* in Chapter 6, *Network Configuration*.

# 5. Dial-in server configuration

SnapGear appliance enables remote and secure access to your office network. This chapter shows how to set up the dial-in features.

Your SnapGear appliance can be configured to receive dial-in calls from remote users/sites. Remote users are individual users (e.g. telecommuters) who connect directly from their client workstations to dial into modems connected to the serial ports on the SnapGear appliance. Remote site dial-in connections can be LAN-to-LAN connections, where a router at a remote site establishes a dial-in link using a modem connected to the SnapGear appliance.

The SnapGear appliance's dial-in facility establishes a PPP connection to the remote user or site. Dial-in requests are authenticated by usernames and passwords verified by the SnapGear appliance. Once authenticated, remote users and sites are connected and have the same access to the LAN resources as a local user.

***Note***

*Not all SnapGear appliances support the RAS (Remote Access Server) functions in this section.*

*The SnapGear appliance Models SOHO+, PRO and PRO+ support up to two dial-in connections. The SnapGear appliance models LITE2, LITE2+, SME530, SME550, SME570 and SME575 support a single dial-in connection.*

To configure the SnapGear appliance for a dial-in connection:

1. Attach an external modem to the appropriate SnapGear appliance serial port (*COM*). On the SnapGear PRO+, you may use the internal modem for dial-in.

2. If necessary, enable and configure the selected SnapGear appliance serial (*COM*) port for dial-in as detailed in *Dial-in Setup*.

3. Set up and configure user dial-in accounts for each person or site requiring dial-in access.

You can also apply filtering to dial-in connections, as detailed in Chapter 7, *Firewall.*

# Dial-in setup

The following figure shows the dial-in setup:

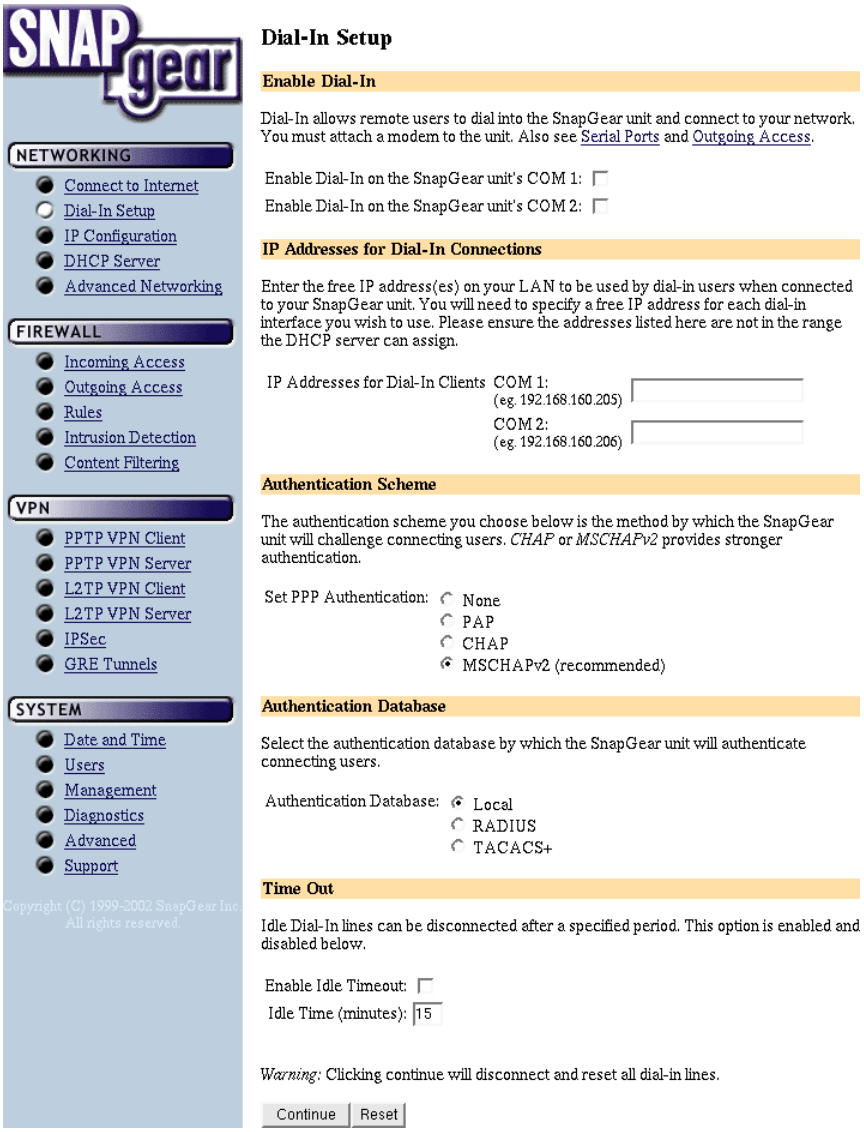

NETWORKING
Connect to Internet
Dial-In Setup
IP Configuration
DHCP Server
Advanced Networking
FIREWALL
Incoming Access
Outgoing Access
Rules
Intrusion Detection
Content Filtering
VPN
PPTP VPN Client
PPTP VPN Server
L2TP VPN Client
L2TP VPN Server
IPSec
GRE Tunnels
SYSTEM
Date and Time
Users
Management
Diagnostics
Advanced
Support
Dial-In Setup
Enable Dial-In
Dial-In allows remote users to dial into the SnapGear unit and connect to your network. You must attach a modem to the unit. Also see Serial Ports and Outgoing Access.
Enable Dial-In on the SnapGear unit's COM 1:
Enable Dial-In on the SnapGear unit's COM 2:
IP Addresses for Dial-In Connections
Enter the free IP address(es) on your LAN to be used by dial-in users when connected to your SnapGear unit. You will need to specify a free IP address for each dial-in interface you wish to use. Please ensure the addresses listed here are not in the range the DHCP server can assign.
IP Addresses for Dial-In Clients
COM 1: (eg. 192.168.160.205)
COM 2: (eg. 192.168.160.206)
Authentication Scheme
The authentication scheme you choose below is the method by which the SnapGear unit will challenge connecting users. CHAP or MSCHAPv2 provides stronger authentication.
Set PPP Authentication:
None
PAP
CHAP
MSCHAPv2 (recommended)
Authentication Database
Select the authentication database by which the SnapGear unit will authenticate connecting users.
Authentication Database:
Local
RADIUS
TACACS+
Time Out
Idle Dial-In lines can be disconnected after a specified period. This option is enabled and disabled below.
Enable Idle Timeout:
Idle Time (minutes): 15
Warning: Clicking continue will disconnect and reset all dial-in lines.
Continue
Reset

**Figure 5.1 Dial-in setup**

To enable and configure Dial-In server for the SnapGear appliance, select **Dial-In Setup** from the **Networking** menu. The following table describes the fields in the **Dial-In Setup** screen and explains how to enable and configure dial-in access on a SnapGear appliance COM port.

| Field | Description |
|---|---|
| Enable Dial-in | To enable and configure dial-in, check the relevant COM port box. The selected port is now available for dial-in access. If no COM port is selected, all dial-in attempts will be blocked.<br>The current dial-in status of all COM ports is displayed. If dial-in is already enabled, the checkbox displays a bold or shaded check mark. If dial-in is not enabled, the checkbox is clear<br>Note: A port enabled for dial-in cannot be used simultaneously for dial-out activities (e.g. dial-on-demand Internet connection). If a port was previously set up for Internet access and is later enabled for dial-in, the Internet access function is disabled.<br>This is not displayed for SME570 and SME575 models. |
| IP Addresses for Dial-in users | Dial-in users must be assigned local IP addresses to access the local network. Specify a free IP address from your local network that each dial-up client will use when connecting to the SnapGear appliance. |
| Authentication Scheme | The authentication scheme is the method the SnapGear appliance uses to challenge users dialing into the network. Dial-in clients must be configured to use the selected authentication scheme.<br>• **MSCHAPv2** is the most secure, and is the only option that also supports data encryption.<br>• **CHAP** is less secure.<br>• **PAP** (although more common) is even less secure.<br>• **None** means that no username/password authentication is required for dial-in. |
| Authentication Database | The authentication database is used to verify the username and password received from the dial-in client.<br>• **Local** means the dial-in user accounts created on the SnapGear appliance. You will need to created user accounts as described below. This can be used with any authentication scheme.<br>• **RADIUS** means an external RADIUS server. You will be prompted to enter the server IP address and password. This can be used with any authentication scheme, provided that the RADIUS server also supports it.<br>• **TACACS+** means an external TACACS+ server. You will be prompted to enter the server IP address and password. This can only be used with the **PAP** authentication scheme. |

| | |
|---|---|
| Idle Timeout | If a dial-in connection remains inactive, it can be automatically disconnected after a specified time period. Selecting **Enable idle timeout** will disconnect idle connections after 5 minutes. **Idle time** can be set between 0 – 99 minutes. |

After enabling and configuring the selected SnapGear appliance COM ports/Modem to support dial-in, click **Continue** to create and configure the dial-in user accounts.

# Dial-in user accounts

User accounts must be set up before remote users can dial-into the SnapGear appliance. The following figure shows the Dial-in user account creation:

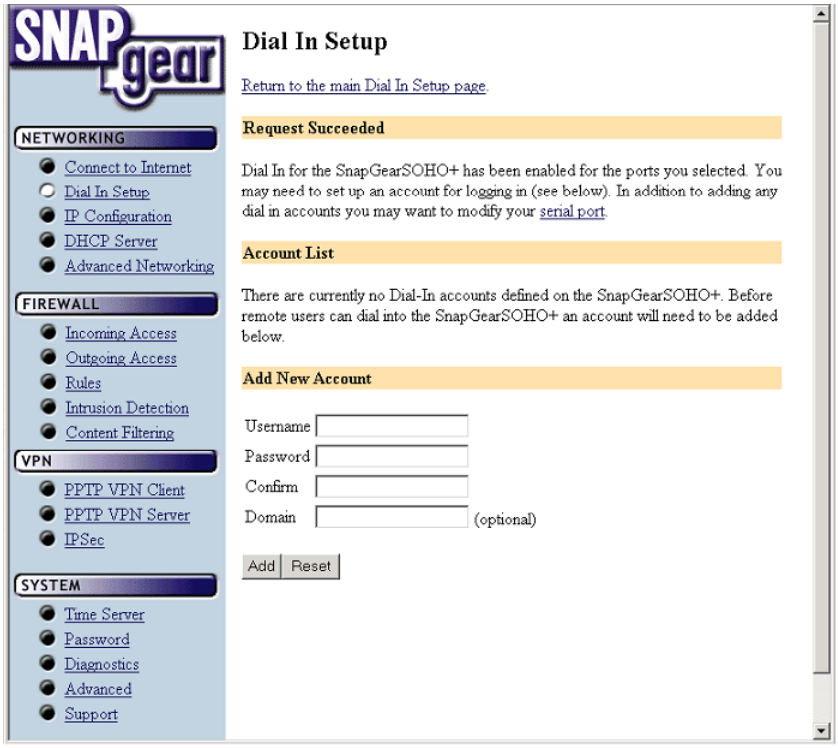



**Figure 5.2 Dial-in user account creation**

The field options in *Add New Account* are shown in the following table:

| Field | Description |
|---|---|
| Username | Username for dial-in authentication only. The name is case-sensitive (e.g. *Jimsmith* is different to *jimsmith*). |
| Password | Password for the remote dial-in user. |
| Confirm | Re-enter the password to confirm. |
| Domain | If your network has a Windows NT server, you can attach a domain name to your dial-in remote user accounts. This field is optional and can be left blank. |

The following figure shows the user maintenance screen:

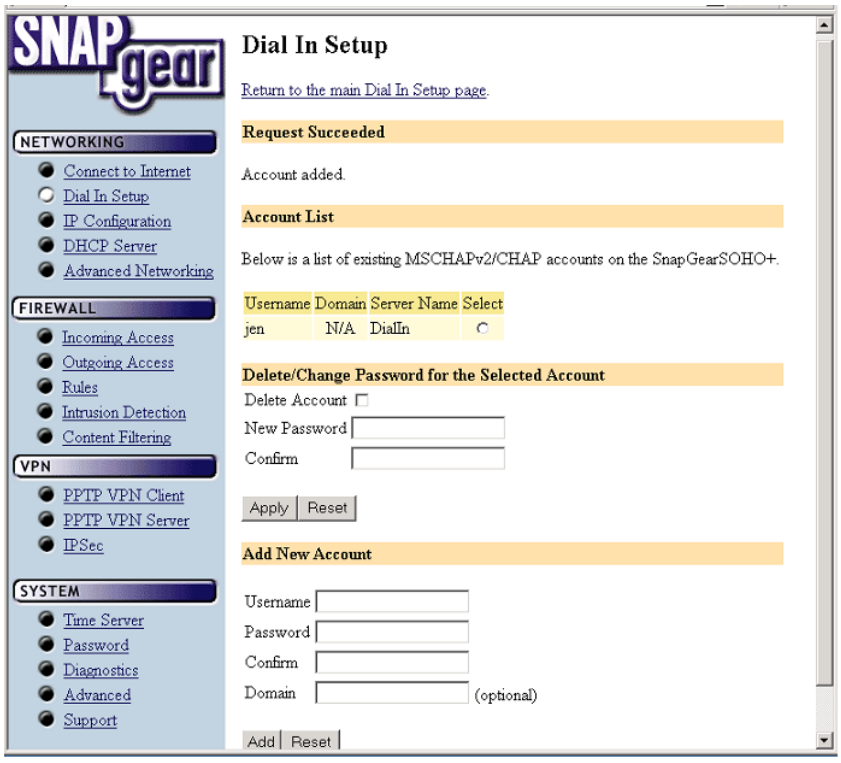



**Figure 5.3 User maintenance screen**

## Account list

As new dial-in user accounts are added, they are displayed on the updated Account List. To modify a password for an existing account, select the account in the Account List and enter the new password in the **New Password** and **Confirm** fields. Click **Apply** under the **Delete or Change Password for the Selected Account** heading, or click **Reset** if you make a mistake.

To delete an existing account, select the account in the **Account List** and check **Delete** under the **Delete or Change Password for the Selected Account** heading. If changes to the user account are successful, the change is shown on the **Dial-in Setup** screen . If the change is unsuccessful, an error is reported as shown in the following figure:

SNAPgear
NETWORKING
Connect to Internet
Dial In Setup
IP Configuration
DHCP Server
Advanced Networking
FIREWALL
Incoming Access
Outgoing Access
Rules
Intrusion Detection
Content Filtering
VPN
PPTP VPN Client
Dial In Setup
Return to the main Dial In Setup page.
Error
Warning: The SnapGearSOHO+ encountered the following problem with the last request:
Password/verify field mismatch.
Your request failed to meet the above requirement. As a result of the above error, your last request has been ignored. Try your request again with amended data.
Account List
Below is a list of existing MSCHAPv2/CHAP accounts on the SnapGearSOHO+.
Username Domain Server Name Select
jen N/A DialIn

**Figure 5.4 Dial-in password error**

When you have finished adding and modifying user account details, you can configure other SnapGear appliance functions by selecting the appropriate item from the **Network** or **System** menus. You can also apply packet filtering to the dial-in service as detailed in Chapter 7, *Firewall*.

***Warning***

*If you have enabled a SnapGear appliance COM port/Modem for dial-in, this port cannot be used simultaneously for dial-out activities (e.g. dial-on-demand Internet connection). If a port is set-up for Internet access, and is later enabled for dial-in, the Internet access function is automatically disabled.*

# Remote user configuration

Remote users can dial-in using the SnapGear appliance using the standard Windows **Dial-Up Networking** software. Set up a new dial-out connection on the remote PC to dial the phone number of the modem connected to the SnapGear appliance COM port.

After the dial-in is connected, users can access all network resources as if they were a local user.

For Windows 95 and Windows 98:

From the **Dial-Up Networking** folder, double-click **Make New Connection** and enter the ***Connection Name*** for your new dial-in connection as shown in the following figure:

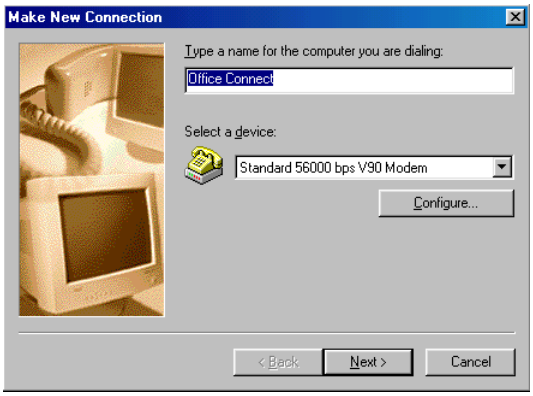



**Figure 5.5 Make new connection screen**

Select the modem to use from the **Select a device** pull down menu.

Click **Next** and enter the phone number of the modem connected to the SnapGear appliance.

Click **Finish**.

An icon is displayed in Dial-Up Networking with your Connection Name. Right click the icon once, and then click **File** and **Properties** and click the **Server Types** tab as shown in the following figure:

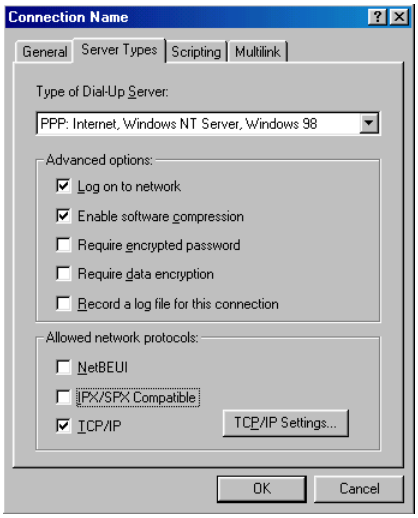



**Figure 5.6 Server types**

Check the **Log on to network** and **Enable software compression** checkboxes. If your SnapGear appliance dial-in server requires *MSCHAP-2* authentication, you also need to check the **Require encrypted password** checkbox. Leave all other **Advanced Options** unchecked.

Select the **TCP/IP** network protocols from the **Allowed network protocols** list.

***Warning***

*Do not select NetBEUI or IPX. If an unsupported protocol is selected, an error message is returned when attempting to connect.*

Click **TCP/IP Settings** and confirm that the **Server Assigned IP Address**, **Server Assigned Name**, **Server Address**, **Use IP Header Compression** and **Use Default Gateway on Remote Network** are all checked and click **OK**.

Dial-in and log on to the remote SnapGear appliance by double-clicking the *Connection Name* icon. You need to enter the **Username** and the **Password** that was set up for the SnapGear appliance dial-in account as shown in the following figure:

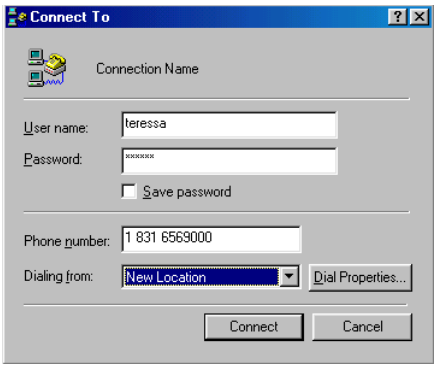



**Figure 5.7 Connect to dialogue box**

## Windows 2000

To configure a remote access connection on a Windows 2000 computer, click **Start**, **Settings**, **Network and Dial-up Connections** and select **Make New Connection.**

The network connection wizard will guide you through setting up a remote access connection:

Network Connection Wizard
Welcome to the Network Connection Wizard
Using this wizard you can create a connection to other computers and networks, enabling applications such as e-mail, Web browsing, file sharing, and printing.
To continue, click Next.
< Back
Next >
Cancel

**Figure 5.8 Network connection wizard**

Click **Next** to continue.

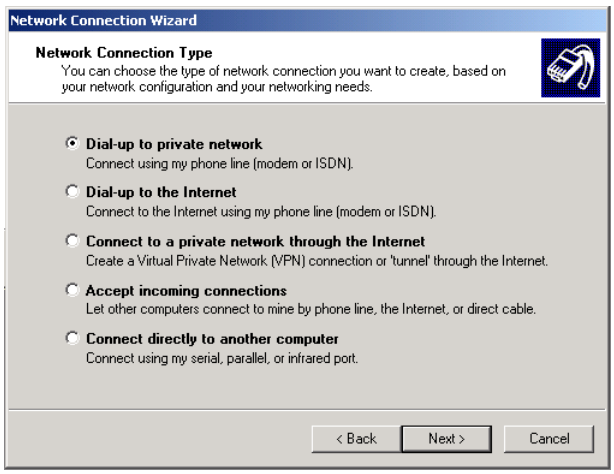

Network Connection Wizard
Network Connection Type
You can choose the type of network connection you want to create, based on your network configuration and your networking needs.
Dial-up to private network
Connect using my phone line (modem or ISDN).
Dial-up to the Internet
Connect to the Internet using my phone line (modem or ISDN).
Connect to a private network through the Internet
Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.
Accept incoming connections
Let other computers connect to mine by phone line, the Internet, or direct cable.
Connect directly to another computer
Connect using my serial, parallel, or infrared port.
< Back
Next >
Cancel

**Figure 5.9 Connection type**

Select **Dial-up to private network** as the connection type and click **Next** to continue.

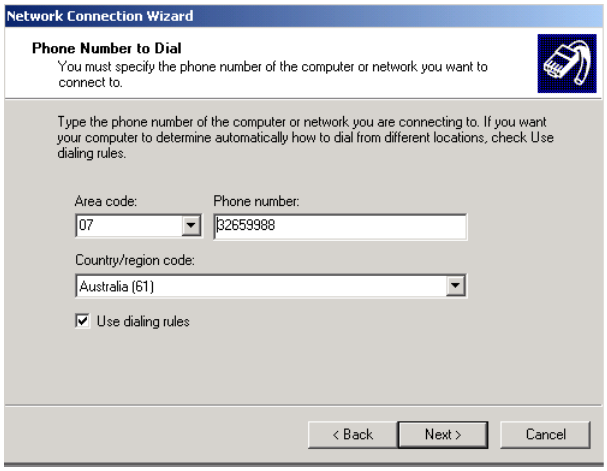

Network Connection Wizard
Phone Number to Dial
You must specify the phone number of the computer or network you want to connect to.
Type the phone number of the computer or network you are connecting to. If you want your computer to determine automatically how to dial from different locations, check Use dialing rules.
Area code:
Phone number:
07
32659988
Country/region code:
Australia (61)
Use dialing rules
< Back
Next >
Cancel

**Figure 5.10 Phone number to dial**

Tick **Use dialing rules** to enable you to select a country code and area code. This feature is useful when using remote access in another area code or overseas.

Click **Next** to continue.

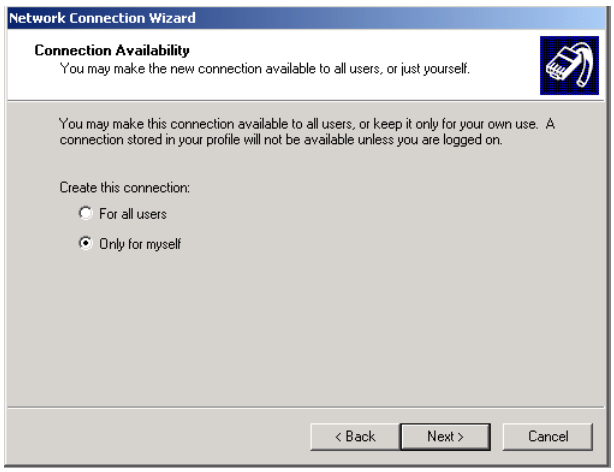

Network Connection Wizard
Connection Availability
You may make the new connection available to all users, or just yourself.
You may make this connection available to all users, or keep it only for your own use. A connection stored in your profile will not be available unless you are logged on.
Create this connection:
For all users
Only for myself
< Back
Next >
Cancel

**Figure 5.11 Connection availability**

Select the option **Only for myself** to make the connection only available for you. This is a security feature that will not allow any other users who log onto your machine to use this remote access connection:

Network Connection Wizard
Completing the Network Connection Wizard
Type the name you want to use for this connection:
Office Connect
To create this connection and save it in the Network and Dial-up Connections folder, click Finish.
To edit this connection in the Network and Dial-up Connections folder, select it, click File, and then click Properties.
Add a shortcut to my desktop
< Back
Finish
Cancel

**Figure 5.12 Connection name**

Enter a name for the connection and click **Finish** to complete the configuration. By ticking **Add a shortcut to my desktop,** an icon for the remote connection will appear on the desktop.

To launch the new connection, double-click on the new icon on the desktop, and the remote access login screen will appear as in the next figure. If you did not create a desktop icon, click **Start, Settings, Network and Dial-up Connections** and select the appropriate connection and enter the username and password set up for the SnapGear appliance dial-in account.

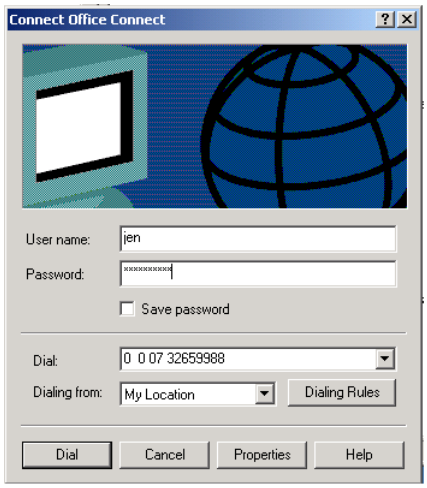



**Figure 5.13 Remote access login screen**

# 6. Network configuration

This chapter describes the **IP Configuration** and **DHCP Server** options, as well as the **Advanced Networking** features of the SnapGear appliance.

***Note***

*This section is slightly different for SME570 and SME575 models. Refer to Chapter 4,* Network Setup and DMZ.

## IP configuration

Users can set the IP address configuration for both the LAN and Internet interfaces by selecting **IP Configuration** from the **Networking** menu as shown in the following figure:

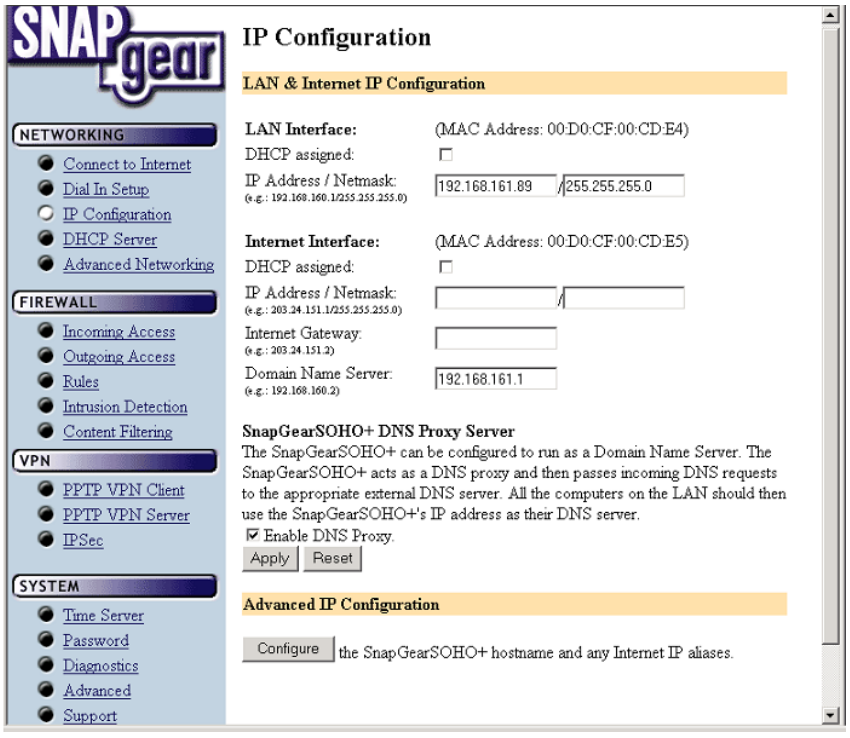



**Figure 6.1 IP configuration**

## LAN Interface

To configure the LAN Interface of the SnapGear appliance, select either a dynamically or statically assigned IP address. If the LAN interface of your SnapGear appliance gets its IP address from a DHCP server on your local network, then check **DHCP assigned**.

For a static IP address on the LAN interface, enter the **IP Address** and **Netmask** in the fields provided. You must enter a static IP address if the SnapGear appliance will act as the DHCP server on your local network.

## Internet Interface

If your SnapGear appliance is configured for a **Direct Connection** to the Internet, you must also set the IP address for the Internet Interface. Check **DHCP assigned** if the IP address of the Internet Interface is set via a DHCP server, or enter the **IP Address** and **Netmask** if you have a static address for the Internet interface.

Enter the IP address of default gateway in the **Internet Gateway** field. The SnapGear appliance will send all packets not destined for the local network to this machine.

Enter the IP address of the DNS Server that the SnapGear appliance will use to resolve domain names in the **Domain Name Server** field. This is only required if the SnapGear appliance is configured with a static IP address on the Internet interface and does not automatically get its DNS server address. Multiple DNS addresses may be entered separated by commas.

## DNS Proxy

The SnapGear appliance can also be configured to run as a Domain Name Server. The SnapGear appliance acts as a **DNS Proxy** and passes incoming DNS requests to the appropriate external DNS server. If this is enabled, all the computers on the LAN should specify the IP address of the SnapGear appliance as their DNS server.

## Bridging

The bridging on the SnapGear appliance is set up to allow users to create transparent Ethernet bridges over IPSec tunnels. This is useful because:

- It allows users to transmit IPX/SPX over a VPN, something that is not supported by other VPN vendors.
- It allows users to transmit DHCP to remote sites this ensures that they are under better control.

- It allows users to make use of protocols that do not work well in a WAN environment (e.g. *netbios*).

The bridging support, at this stage, does not extend to bridging between Ethernet interfaces, or bridging between PPPoE interfaces.

The first step is setting up a *host to host* IPSec VPN connection. Information regarding setting up a host to host VPN connection can be found in the IPSec section of this manual.

Check **Enable bridging** and click **Apply**. You will need to reboot for this to take effect.

***Warning***

*The unit will take up to 30 seconds longer than normal to reboot after bridging has been enabled.*

# Advanced IP configuration

The following figure shows the advanced IP configuration:

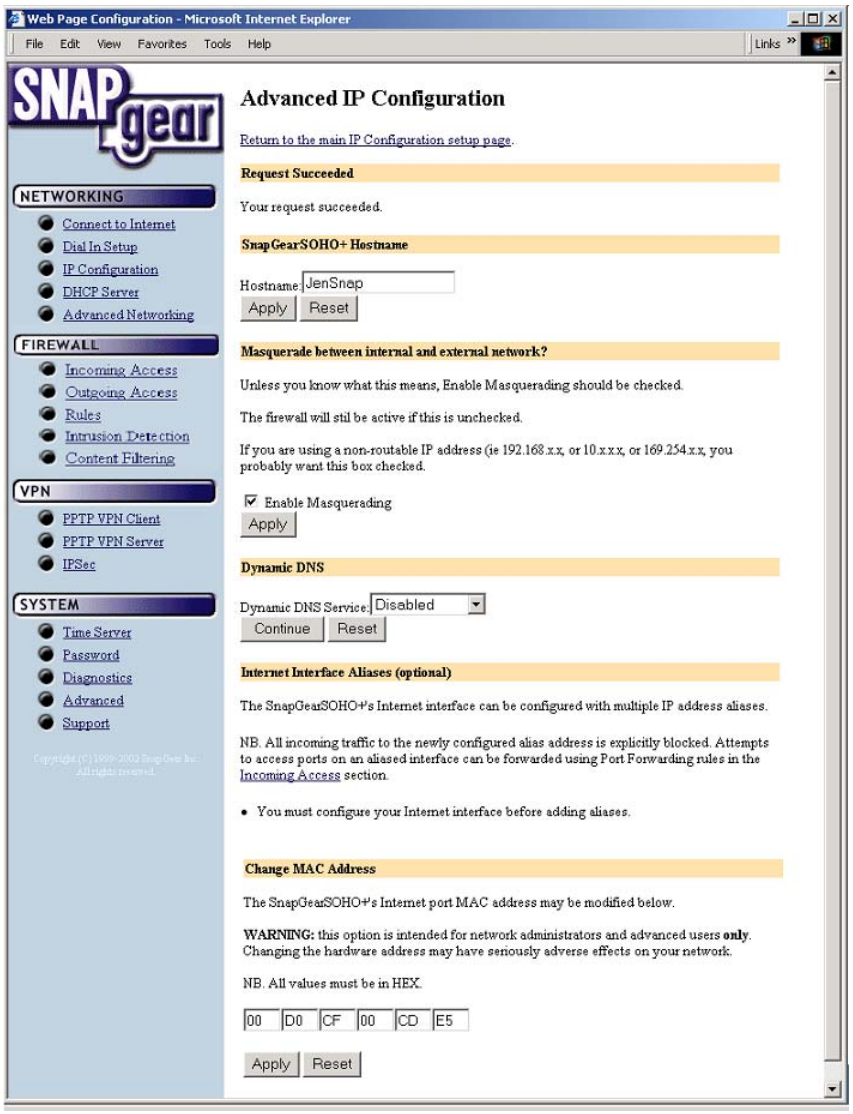

Web Page Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links
SNAPgear
NETWORKING
Connect to Internet
Dial In Setup
IP Configuration
DHCP Server
Advanced Networking
FIREWALL
Incoming Access
Outgoing Access
Rules
Intrusion Detection
Content Filtering
VPN
PPTP VPN Client
PPTP VPN Server
IPSec
SYSTEM
Time Server
Password
Diagnostics
Advanced
Support
Advanced IP Configuration
Return to the main IP Configuration setup page.
Request Succeeded
Your request succeeded.
SnapGearSOHO+ Hostname
Hostname: JenSnap
Apply Reset
Masquerade between internal and external network?
Unless you know what this means, Enable Masquerading should be checked.
The firewall will stil be active if this is unchecked.
If you are using a non-routable IP address (ie 192.168.x.x, or 10.x.x.x, or 169.254.x.x, you probably want this box checked.
Enable Masquerading
Apply
Dynamic DNS
Dynamic DNS Service: Disabled
Continue Reset
Internet Interface Aliases (optional)
The SnapGearSOHO+'s Internet interface can be configured with multiple IP address aliases.
NB. All incoming traffic to the newly configured alias address is explicitly blocked. Attempts to access ports on an aliased interface can be forwarded using Port Forwarding rules in the Incoming Access section.
You must configure your Internet interface before adding aliases.
Change MAC Address
The SnapGearSOHO+'s Internet port MAC address may be modified below.
WARNING: this option is intended for network administrators and advanced users only. Changing the hardware address may have seriously adverse effects on your network.
NB. All values must be in HEX.
00 D0 CF 00 CD E5
Apply Reset

**Figure 6.2 Advanced IP configuration**

## Hostname

The **Hostname** is a descriptive name for the SnapGear appliance on the network.

## Network Address Translation (NAT/Masquerading)

The SnapGear appliance can utilize *IP Masquerading* (a simple form of Network Address Translation, or NAT) where users on the local network effectively share a single external IP address. Masquerading allows insiders to get out, without allowing outsiders in. By default, the Internet interface is setup to Masquerade.

Masquerading has the following advantages:

- Added security because machines outside the local network only know the gateway address.
- All machines on the local network can access the Internet using a single ISP account.
- Only one public IP address is used and is shared by all machines on the local network. Each machine has its own private IP address.

SnapGear recommends setting **Masquerade** on the Internet interface.

On SME570 and SME575 models, you may also choose to enable masquerading between the **LAN** and **DMZ** interfaces.

## Interface aliases

**Interface aliases** allow the SnapGear appliance to respond to multiple IP addresses on its LAN, Internet and DMZ interfaces. For Internet and DMZ aliased interfaces, you must also setup appropriate **Packet Filtering** rules to allow traffic on these interfaces to be passed onto the local network.

## Change MAC address

On rare occasions it may be necessary to change the Ethernet hardware or **MAC Address** of your SnapGear appliance. The MAC address is a globally unique address and is specific to a single SnapGear appliance. It is set by the manufacturer and should not normally be changed. However, you may need to change it if your ISP has configured your ADSL or cable modem to only communicate with a device with a known MAC address.

# DHCP server

To help keep your network design as simple as possible, your SnapGear appliance can act as a DHCP server for machines on your local network. To configure your SnapGear appliance as a DHCP server, you must set a static IP address and netmask on the LAN or DMZ Interface (see the section called *Network Configuration*).

The DHCP server allows the automatic distribution of IP, gateway, DNS and WINS addresses to hosts running DHCP clients on the LAN and/or DMZ interfaces. To configure the DHCP server click the **DHCP Server** link in the **Networking** section of the left menu bar. A page similar to the following will be displayed.

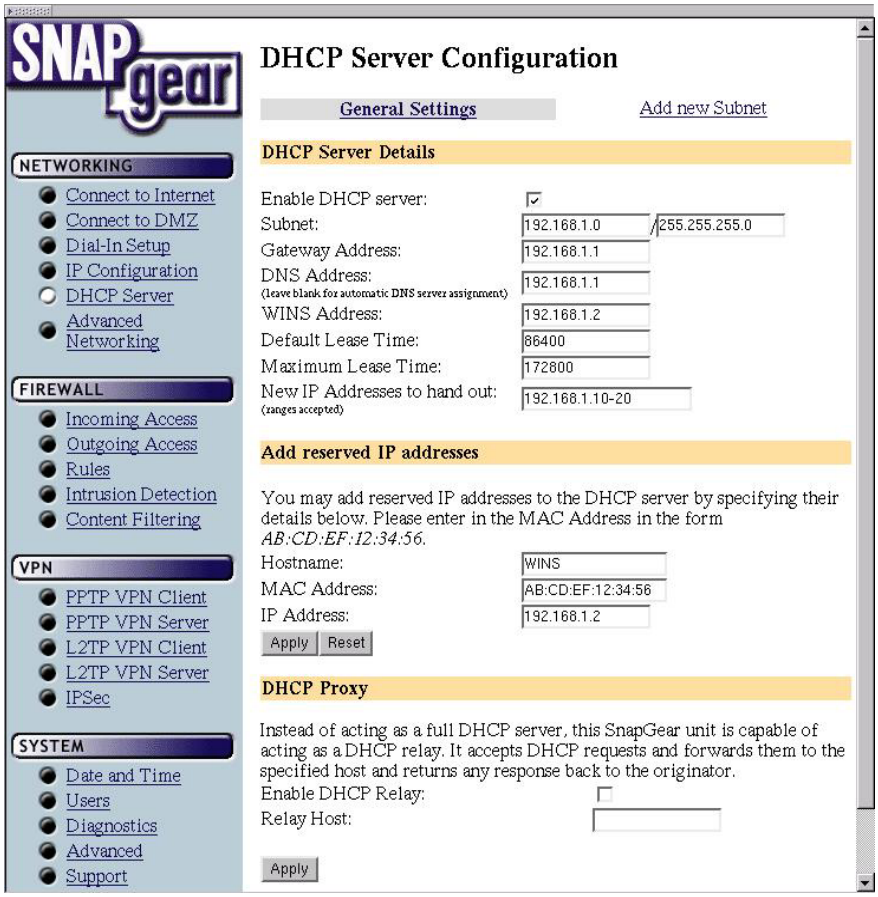



**Figure 6.3 DHCP server configuration**

To configure the DHCP Server, follow these instructions.

- Check the **Enable DHCP Server** checkbox.
- Enter the **Subnet** and netmask of the IP addresses to be distributed.
- Enter the **Gateway Address** that the DHCP clients will be issued with. If this field is left blank, the SnapGear's IP address will be used.
- Enter the **DNS Address** that the DHCP clients will be issues with. If this field is left blank, the SnapGear's IP address will be used. Leave this field blank for automatic DNS server assignment. If your SnapGear appliance is configured for DNS masquerading, you should either leave this field blank, or enter the IP address of the LAN interface of the SnapGear appliance.
- Enter IP address of the WINS server to be distributed to DHCP clients in the **WINS Address** field.
- Enter the **Default Lease Time** and **Maximum Lease Time** in seconds. The lease time is the time that a dynamically assigned IP address is valid.
- Enter the IP address or range of IP addresses to be issued to DHCP clients in the **New IP Addresses to hand out** field.

The DHCP Server can also reserve IP addresses for particular hosts, identifying them by hostname and MAC address. To reserve an IP address for a certain host, configure the following in the **Add reserved IP address** section.

- Enter the **Hostname** of the DHCP client.
- Enter the **MAC address** of the DHCP client.
- Enter the reserved **IP address** for the DHCP client.

To take advantage of the SnapGear appliance’s DHCP server functionality, you should configure the other machines on your local network to get their IP addresses dynamically from the SnapGear appliance. Please refer the documentation for the other machines for instructions on how to configure the local network interface.

Click **Apply** to save these settings. A page similar to the following will be displayed.

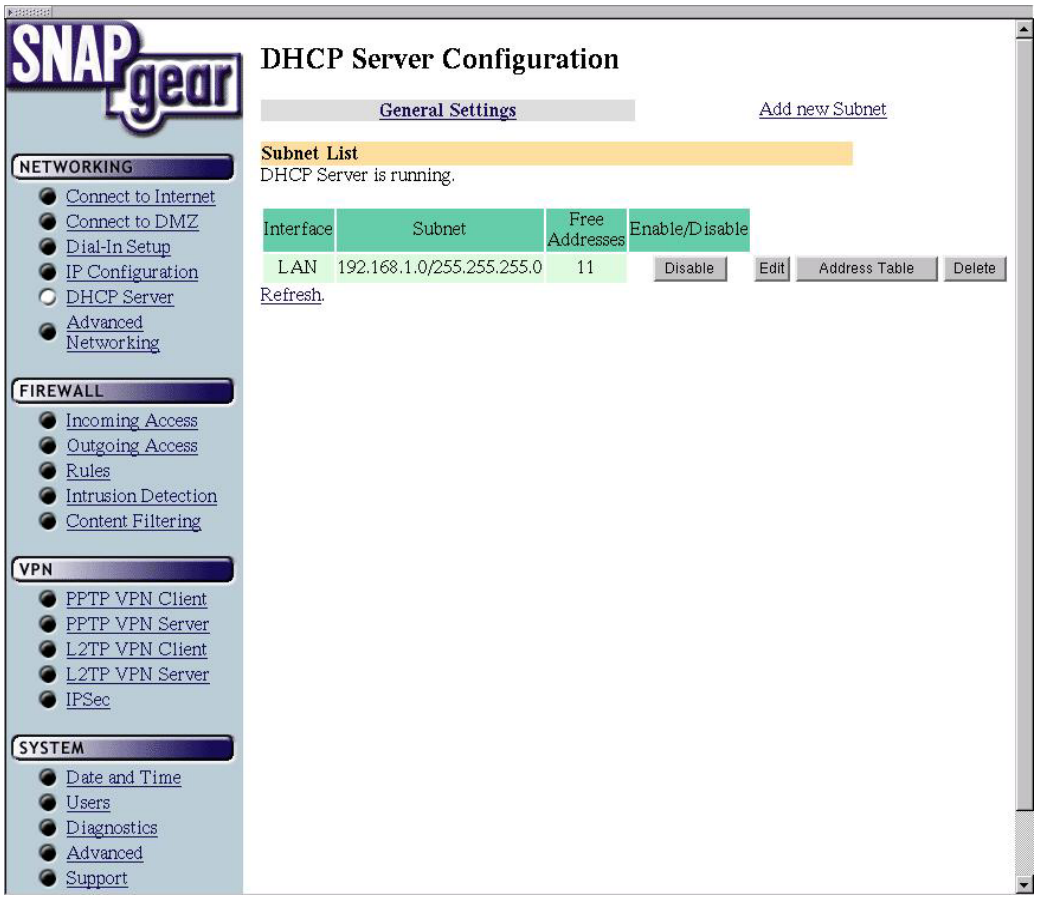



**Figure 6.5 DHCP Subnet List**

## Subnet List

The **Subnet List** will display the status of the DHCP server.

## Interface

Once a subnet has been configured, the interface which the IP addresses will be issued from will be shown in the **Interface** field.

## Subnet

The value shown in this field is the subnet for which the IP addresses distributed will use.

### Free Addresses

This field will contain the number of remaining available IP addresses that can be distributed. You may need to increase the number of IP addresses to hand out if this value is 0.

### Enable/Disable

Each subnet can be enabled or disabled by clicking on the **Enable** or **Disable** button under the **Enable/Disable** heading.

### Edit

The settings for each subnet can be modified by clicking the **Edit** button. You will also have the option to add more IP addresses that can be handed out and add reserved IP addresses as well.

### Address Table

A table listing the status of each IP address that the DHCP server services for the subnet can be viewed by clicking the **Address Table** button.

### Delete

The settings for the subnet can be removed by clicking the **Delete** button.

Clicking the **Address Table** button will display a page similar to the following.

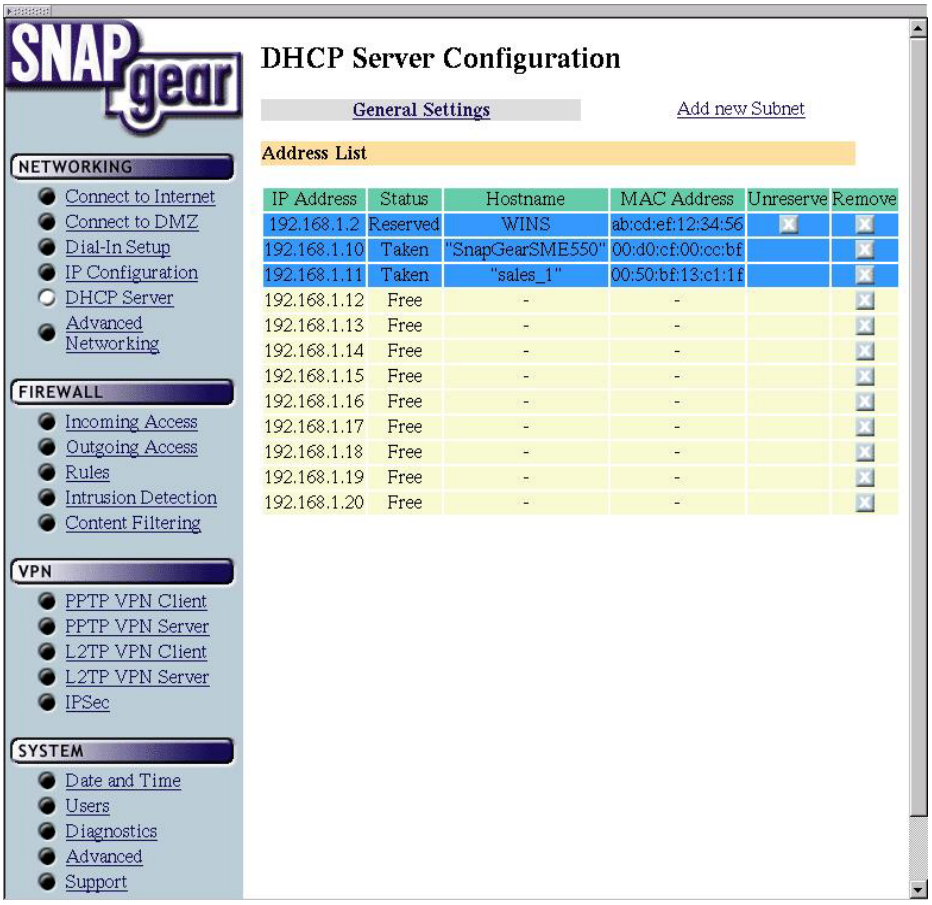



**Figure 6.6 DHCP Address List**

For each IP address that the DHCP server services, the **Status**, **Hostname**, **MAC Address** will be shown. There is also be an option to **Remove** the address and for reserved IP addresses, the added option to **Unreserve** the address. Unreserving the address will allow it to be handed out to any host. The **Status** field will have three possible states. These include:

- **Reserved** - the address is reserved for the particular host defined by hostname and MAC address.
- **Free** - the address is available to be handed out to any DHCP client host.
- **Taken** - the address has been issued to a host.

## DHCP proxy

The DHCP proxy allows the SnapGear unit forward DHCP requests from the LAN to an external server for resolution. This allows both static and dynamic addresses to be given out on the LAN just as running a DHCP server would.

To enable this feature, specify the server which is to receive the forwarded requests in **Relay Host**. This server must also be configured to know and accept requests from the SnapGear unit's LAN. Then check **Enable DHCP Relay** and click **Apply**.

## IP address ranges

IP ranges are fields that allow multiple IP addresses to be specified using a shorthand notation. Four distinct forms of range are acceptable:

1. **a.b.c.d**
2. **a.b.c.d-e**
3. **a.b.c.d-e.f.g.h**
4. **a.b.c.d/e**

The first is simply a single IP address. Thus where ever a range is permitted, a single IP address is too.

The second specifies range of IP address from **a.b.c.d** to **a.b.c.e** inclusive, i.e. you are specifying a range within a C class network or subnet. For example, *192.168.5.15-30* includes 16 IP addresses.

The third form allows the address range to span network and subnet boundaries. All addresses including and between the two specified IP addresses are included in the range. For example, *192.168.5.190-192.168.6.56* includes 123 IP addresses.

The final form allows the range to be specified to cover an entire subnet. The value of **e** specified the number of fix bits in the IP address range. Thus, **a.b.c.d/24** covers the entire C class network/subnet **a.b.c.0** and is equivalent to specifying the range as **a.b.c.0-255** (the value for **d** here can be anything as it is ignored). A range of **a.b.c.d/32** is equivalent to the single IP address **a.b.c.d**. For example, *192.168.12.150/26* is equivalent to the range *192.168.12.128-191* and it includes 64 IP addresses.

# Advanced networking

Users can perform the following diagnostic tasks on the **Advanced Networking** screen:

- Perform a Ping Test.
- Perform a Trace Route Test.
- View the Interface Configuration.
- View the network Route Table.

The advanced networking configuration tasks **Traffic Shaping** and **Additional Routes** are also accessed using the **Advanced Networking** page.

## Traffic shaping

The **Traffic Shaping** feature of your SnapGear appliance allows you to allocate **High, Medium,** or **Low** priority to the following services: domain (tcp), domain (udp), ftp, ftp-data, http, https, imap, irc, nntp, ntp, pop3, smtp, ssh, and telnet.

**Traffic Shaping** provides a level of control over the relative performance of various types of IP traffic. This advanced feature is provided for expert users to fine tune their networks.

## Additional routes

The **Additional routes** feature allows expert users to add additional static routes for the SnapGear appliance. These routes are additional to those created automatically by the SnapGear appliance configuration scripts.

## Route Management

PRO+, SME530, SME550, SME570 and SME575 units can be configured to automatically exchange routing information with other routers. Note that this feature is intended for network administrators adept at configuring route management services.

Check **Enable route management**, select the **Protocol** you wish to use to exchange routes and click **Apply**. Once enabled, the routing manager can be configured by editing **zebra.conf** and ***protocol*d.conf** (e.g. **bgpd.conf**) through **Configuration Files**.

For more information on configuring route management, refer to:
**http://www.zebra.org/**

# 7. Firewall

The SnapGear appliance has a fully featured, stateful firewall. The firewall allows you to control both incoming and outgoing access and to detect intrusion attempts, so that PCs on the office network can have tailored Internet access facilities and be shielded from malicious attacks.

The SnapGear Firewall filters packets at the network layer, determines whether the session packets are legitimate and evaluates the contents of packets at the application layer to provide maximum protection for your private network.

## Incoming access

Click **Incoming Access** on the **Firewall** menu to show the **Incoming Access** configuration page to configure the firewall to:

- Control external access to services provided by the SnapGear appliance itself.
- Control services provided by machines on your local network.

## Administration services

The following figure shows the incoming access configuration page:

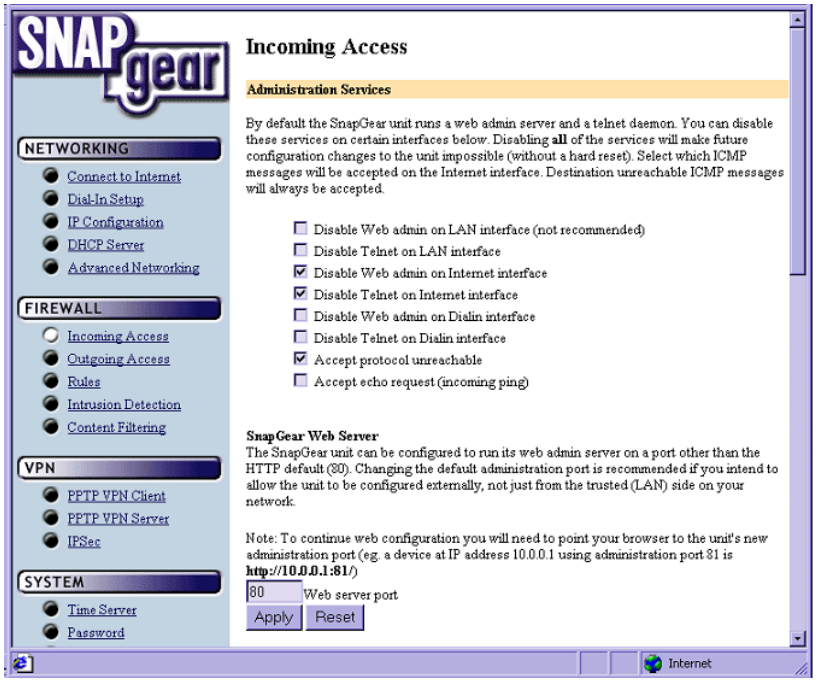

SNAPgear
NETWORKING
Connect to Internet
Dial-In Setup
IP Configuration
DHCP Server
Advanced Networking
FIREWALL
Incoming Access
Outgoing Access
Rules
Intrusion Detection
Content Filtering
VPN
PPTP VPN Client
PPTP VPN Server
IPSec
SYSTEM
Time Server
Password
Incoming Access
Administration Services
By default the SnapGear unit runs a web admin server and a telnet daemon. You can disable these services on certain interfaces below. Disabling all of the services will make future configuration changes to the unit impossible (without a hard reset). Select which ICMP messages will be accepted on the Internet interface. Destination unreachable ICMP messages will always be accepted.
Disable Web admin on LAN interface (not recommended)
Disable Telnet on LAN interface
Disable Web admin on Internet interface
Disable Telnet on Internet interface
Disable Web admin on Dialin interface
Disable Telnet on Dialin interface
Accept protocol unreachable
Accept echo request (incoming ping)
SnapGear Web Server
The SnapGear unit can be configured to run its web admin server on a port other than the HTTP default (80). Changing the default administration port is recommended if you intend to allow the unit to be configured externally, not just from the trusted (LAN) side on your network.
Note: To continue web configuration you will need to point your browser to the unit's new administration port (eg. a device at IP address 10.0.0.1 using administration port 81 is http://10.0.0.1:81/)
80
Web server port
Apply
Reset
Internet

**Figure 7.1 Incoming access configuration**

By default the SnapGear appliance runs a web administration server and a telnet service. Access to these services can be restricted to specific interfaces. For example, you may want to restrict access to the *SnapGear Management Console* web administration pages (**Web Admin**) to machines on your local network. Disallowing all services is not recommended, as this will make future configuration changes impossible unless your SnapGear appliance is reset to the factory default settings.

You can also select the ICMP messages accepted on the Internet interface. For example, if you disallow echo requests (the default for increased security), your SnapGear appliance will not respond to pings on its Internet interface. Destination unreachable ICMP messages are always accepted.

## SnapGear web server

Clicking **Modify** takes you to the page to configure the administrative web server. Here you can change the port on which the server runs. Additionally, the PRO+, SME550, SME570 and SME575 models support SSL encryption to establish secure connections to the *SnapGear Management Console* web administration pages from SSL enabled browsers.

The *SnapGear Management Console* web administration pages are usually accessed on the default HTTP port (i.e. port 80). Change the port number if you are allowing Internet access to the web administration pages. This will hide your web administration pages from casual web surfers who finds your SnapGear appliance on the Internet. After changing the web server port number, you must include the new port number in the URL to access the pages. For example, if you change the web administration to port number 88, the URL to access the web administration will be similar to**:**
**`http://192.168.22.1:88`**

## SnapGear SSL/HTTPS

PRO+, SME550, SME570 and SME575 models only. The current status of the SSL (secure HTTP) support is indicated by **Active**/**Inactive**. Once valid SSL certificates have been uploaded, the SnapGear administrative web server can operate in one of one of 3 different modes.

- Both normal and SSL web access (both HTTP/HTTPS)
- Disable normal access (HTTPS only)
- Disable SSL access (HTTP only)

To access the S*napGear Management Console* administrative web pages securely using SSL encryption, the URL becomes **https://** instead of **http://** (e.g. **`https://10.0.0.1`**).

## Add Local and Private Certificates

PRO+, SME550, SME570 and SME575 models only. **Valid SSL certificates have been uploaded** indicates whether valid certificates are present on the SnapGear appliance (**Yes**/**No**).

If you have purchased or created SSL certificates for a web server, you can upload them to the SnapGear appliance by clicking **Upload**.

Alternately, you can create self-signed certificates internally on the SnapGear unit by following the link to the *SSL Certificate* page.

## SSL Certificate Setup

You can create self-signed certificates on this page, which will enable the SnapGear administrative web server to run in SSL mode.

***Warning***

*Your web browser may give warnings/errors about the authenticity/validity of the certificate, since it is signed by an unknown Certificate Authority.*

Generating certificates is not immediate, and usually takes a few minutes. Exact time will depend on the model of SnapGear appliance you have, and the key size being generated.

You can tell when the certificates are created, the line **Valid SSL certificates have been uploaded** will read **Yes** when the previous page is refreshed.

The SnapGear appliance will need to be rebooted after valid certificates have been uploaded for the administrative web server to use them.

## Port forwarding

The following figure shows the port forwarding configuration:

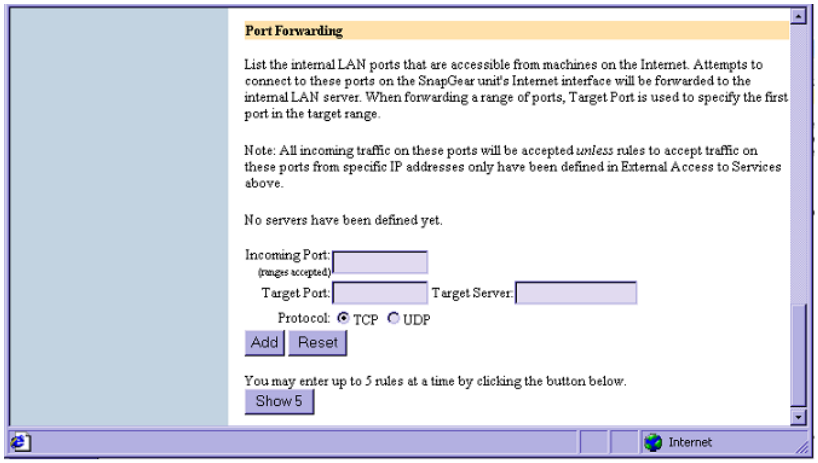

Port Forwarding
List the internal LAN ports that are accessible from machines on the Internet. Attempts to connect to these ports on the SnapGear unit's Internet interface will be forwarded to the internal LAN server. When forwarding a range of ports, Target Port is used to specify the first port in the target range.
Note: All incoming traffic on these ports will be accepted unless rules to accept traffic on these ports from specific IP addresses only have been defined in External Access to Services above.
No servers have been defined yet.
Incoming Port:
(ranges accepted)
Target Port:
Target Server:
Protocol: TCP UDP
Add
Reset
You may enter up to 5 rules at a time by clicking the button below.
Show 5
Internet

**Figure 7.2 Port forwarding configuration**

Port forwarding allows the SnapGear appliance to control access to services provided by machines on your private network from users on the Internet. Requests coming into the SnapGear appliance on the specified **Incoming Port(s)** are forwarded to the **Target Port** on the **Target Server**.

The **Incoming Port** is the port on the SnapGear appliance that will receive the request (the one used by external users establishing the connection). The **Target Server** is the internal machine that is running a server on **Target Port** that will service the incoming connection. **Incoming Port** and **Target Port** are often the same.

If an **Incoming Port** range is specified, e.g. 27960-27970, only the first **Target Port** on the **Target Server** needs to be specified, e.g. 28000. In this example, requests on port 27965 to the SnapGear appliance's Internet IP address will be forwarded to the **Target Server**'s port 28005.

Also note that there is no need to create an entry under **External Access to Services** to allow traffic in on a forwarded port. The SnapGear appliance will make the appropriate firewall modifications automatically. However, you may wish to utilize **Packet Filtering** to restrict access to a forwarded port, e.g. to only allow connections from a specific, trusted external IP address.

# Packet Filtering

By default, your SnapGear appliance allows network traffic as shown in the following table:

| Incoming Interface | Outgoing Interface | Action |
|---|---|---|
| LAN/VPN/Dial-In | Any | Accept |
| DMZ | WAN | Accept |
| DMZ | Any except WAN | Drop |
| WAN | Any | Drop |

You can configure your SnapGear appliance with additional rules to allow or restrict network traffic. These rules can match traffic based on the source and destination address, the incoming and outgoing network interface, and/or the services. Before configuring any rules, you need to define the addresses and service groups. The current addresses, services groups, and rules are all listed on the main **Packet Filtering** page, as shown in the following figure:

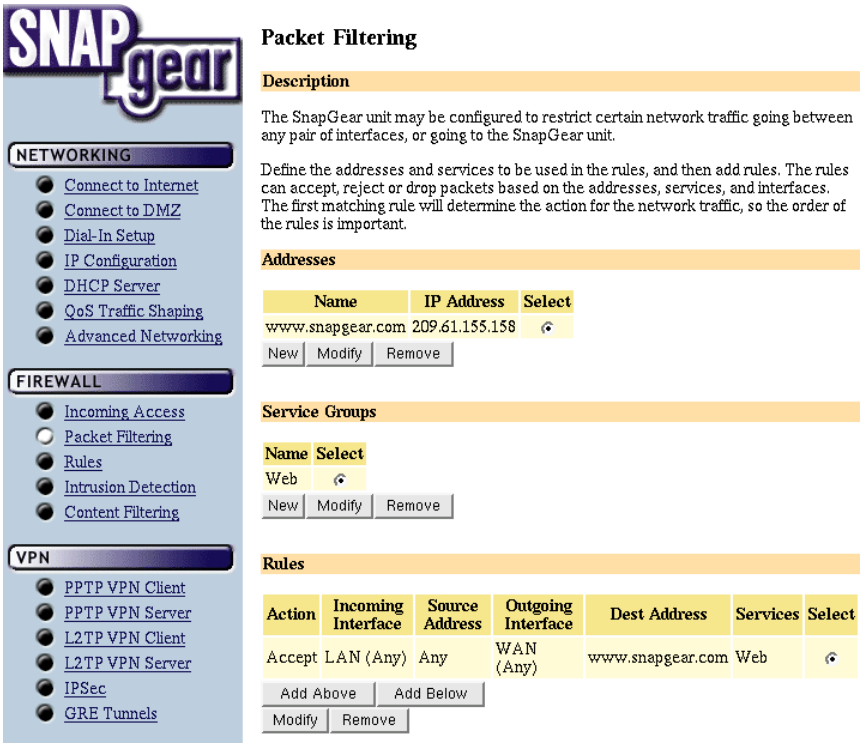



**Figure 7.3 Addresses, service groups and rules**

Adding or modifying an address is shown in the following figure:

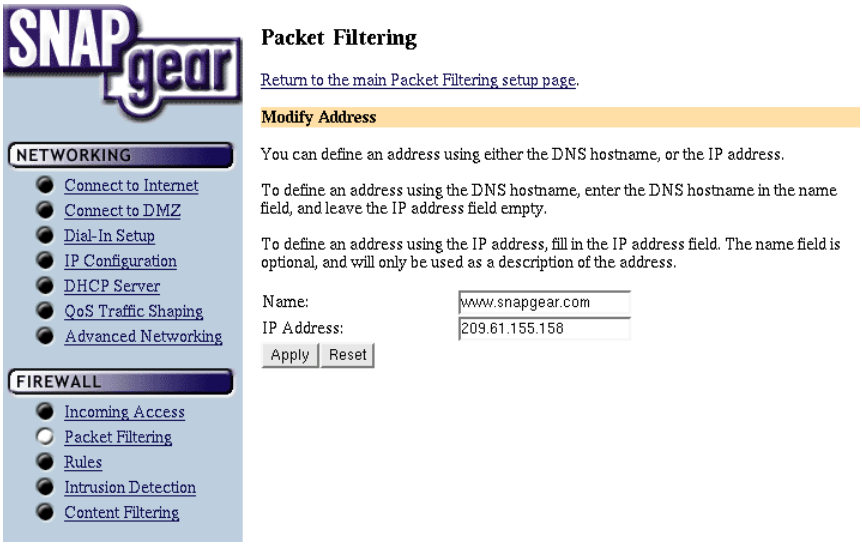

SNAPgear
NETWORKING
Connect to Internet
Connect to DMZ
Dial-In Setup
IP Configuration
DHCP Server
QoS Traffic Shaping
Advanced Networking
FIREWALL
Incoming Access
Packet Filtering
Rules
Intrusion Detection
Content Filtering
Packet Filtering
Return to the main Packet Filtering setup page.
Modify Address
You can define an address using either the DNS hostname, or the IP address.
To define an address using the DNS hostname, enter the DNS hostname in the name field, and leave the IP address field empty.
To define an address using the IP address, fill in the IP address field. The name field is optional, and will only be used as a description of the address.
Name:
www.snapgear.com
IP Address:
209.61.155.158
Apply
Reset

**Figure 7.4 Modifying an address**

You can define an address using either the DNS hostname, or the IP address.

To define an address using the DNS hostname, enter the DNS hostname in the **Name** field, and leave the **IP Address** field empty. The SnapGear appliance will perform a DNS lookup, and fill in the **IP Address** field. If the DNS hostname is invalid, you may need to wait while the DNS lookup times out.

***Warning***

*The DNS lookup is only performed once, when you enter it. If the IP address corresponding to the DNS hostname ever changes, you will need to delete the IP address to force the SnapGear appliance to perform another DNS lookup. This means that this option is not suitable for use with dynamic DNS.*

*Additionally, some DNS hostnames resolve to several IP addresses (eg. www.cnn.com). In this case, you must create an address entry and rule for each of these IP addresses.*

To define an address using the IP address, fill in the **IP Address** field. The **Name** field is optional, and will only be used as a description of the address. Entering a description will make the rules easier to read.

## Service Groups

Adding or editing a service group is shown in the following figure:

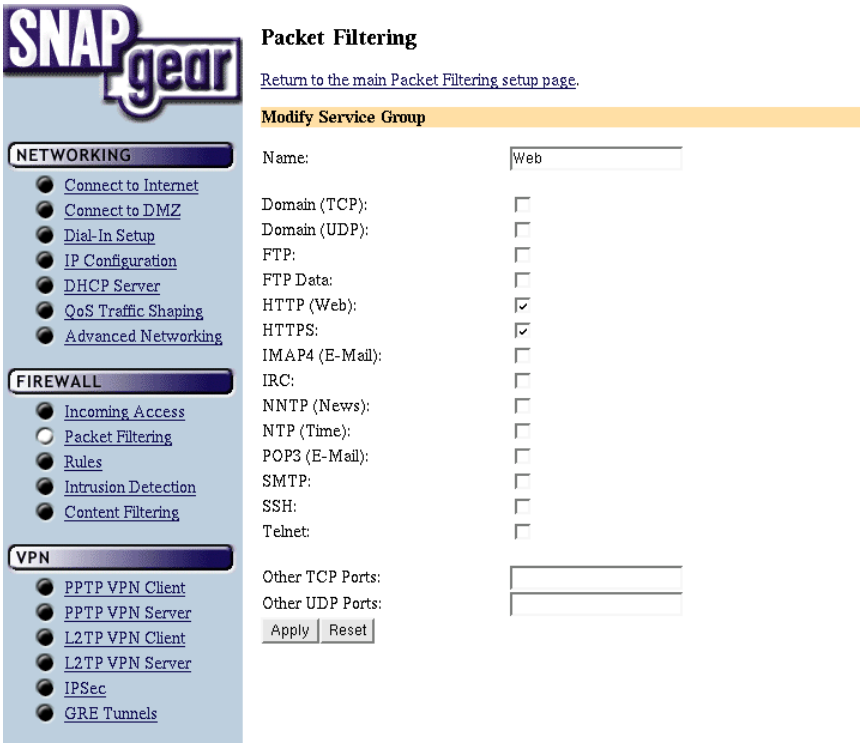



**Figure 7.5 Modifying a service group**

A service group can be used to group together similar services. For example, you can create a group of services that you wish to allow, and then use a single rule to allow them all at once. Select the services from the list of predefined services, or enter the port number to define a custom TCP or UDP service. It is permissible for a service to belong to multiple service groups.

## Rules

Now that the addresses and services have been defined, you can create rules. The first matching rule will determine the action for the network traffic, so the order of the rules is important. You can use the buttons on the **Packet Filtering** page to change the order.

Adding or editing a rule is shown in the following figure:

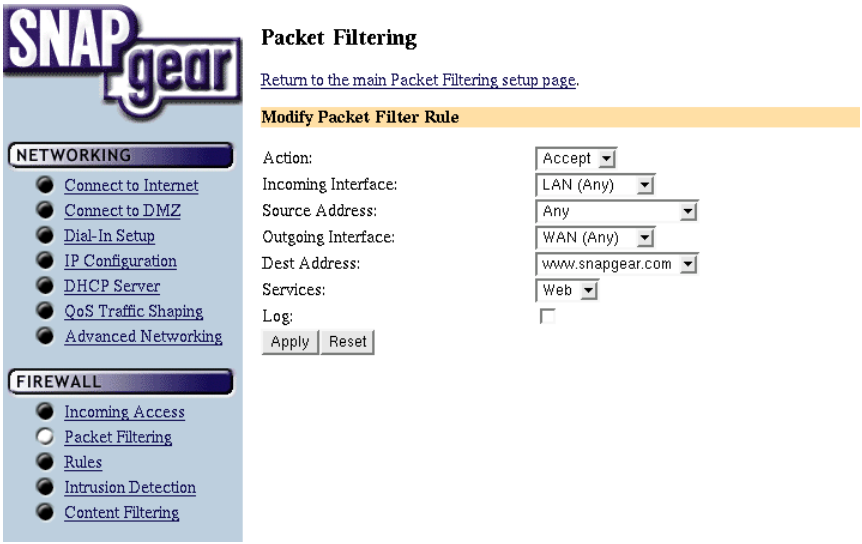



**Figure 7.6 Modfying a rule**

The **Action** specifies what to do if the rule matches.

- **Accept** means to allow the traffic.
- **Drop** means to disallow the traffic.
- **Reject** means to disallow the traffic, but also send an ICMP port unreachable message to the source IP address.
- **None** means to perform no action for this rule. This is useful for a rule that logs packets, but performs no other action. It can also be used to temporarily disable a rule.

The **Incoming Interface** is the interface that the SnapGear appliance received the network traffic on.

The **Outgoing Interface** is the interface that the SnapGear appliance will route the network traffic out. None will match network traffic that is destined for the SnapGear appliance itself. This is useful for controlling access to services provided by the SnapGear appliance, such as the SnapGear Management Console.

The **Log** option controls whether to log the first packet of the connection. The prefix of the log message will be *PF Accept*, *PF Drop*, *PF Reject*, or *PF None*, based on the action for the rule.

# Firewall rules

The **Firewall Rules** configuration page allows firewall experts to view the current firewall rules and add custom firewall rules.

To access this page, click **Rules** in the **Firewall** menu. Only experts on firewalls and *iptables* rules will be able to add effective custom firewall rules. Configuring the SnapGear firewall via the **Incoming Access** and **Outgoing Access** configuration pages is adequate for most applications.

## Allowing individual ports in bridged mode

Enter a rule similar to the following to allow a port through to the internal machine when in bridged mode. Note that this rule must be entered as a single line without the carriage return before *–dport*.

```
iptables -I ExtAcc -p PROTOCOL -i eth1 --sport 1024:65535
      --dport PORTNUMBER -j ACCEPT
```

Where *PROTOCOL* is either **tcp** or **udp**, and *PORTNUMBER* is the port on the machine behind the firewall bridge to which you want to allow access.

# Intrusion detection and blocking

The following figure shows the Intrusion Detection and Blocking (IDB) configuration:

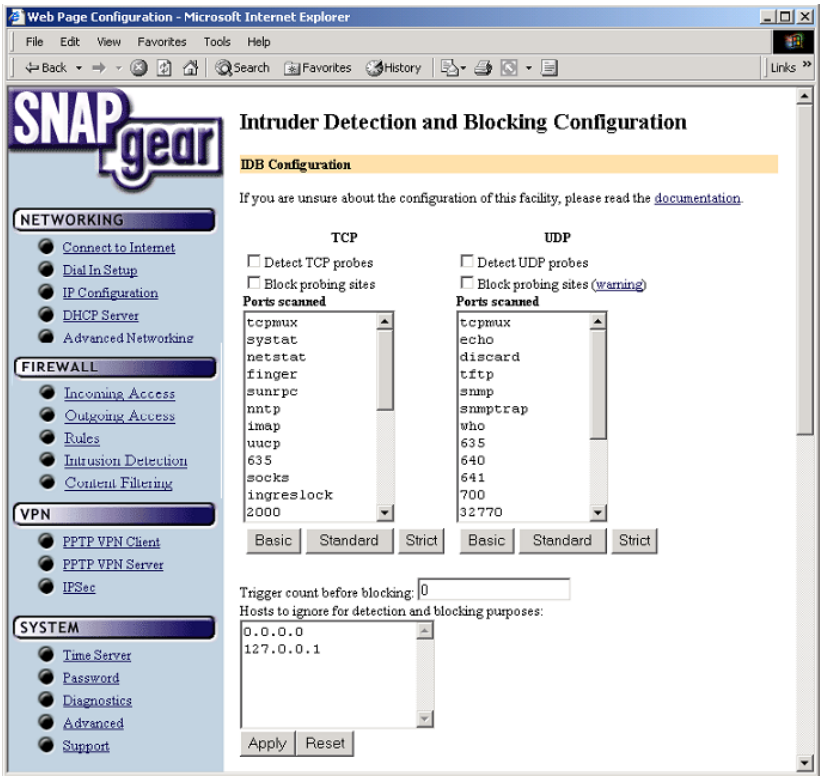



**Figure 7.7 Intrusion detection and blocking configuration**

IDB operates by offering a number of services to the outside world that are monitored for connection attempts. Remote machines attempting to connect to these services generate a system log entry providing details of the access attempt, and the access attempt is denied.

Because network scans often occur before an attempt to compromise a host, you can also deny all access from hosts that have attempted to scan monitored ports. To enable this facility, select one or both of the block options and these hosts are automatically blocked once detected.

The list of monitored network ports can be freely edited. Several shortcut buttons also provide pre-selected lists of services to monitor. The **basic** button installs a bare bones selection of ports to monitor while still providing sufficient coverage to detect many intruder scans. The **standard** option extends this coverage by introducing additional monitored ports for early detection of intruder scans. The **strict** button installs a comprehensive selection of ports to monitor and should be sufficient to detect most scans.

The **trigger count** specifies the number of times a host is permitted to attempt to connect to a monitored service before being blocked. This option only takes effect when one of the previous blocking options is enabled. The trigger count value should be between 0 and 2 (o represents an immediate blocking of probing hosts). Larger settings mean more attempts are permitted before blocking and although allowing the attacker more latitude, these settings will reduce the number of false positives.

The ignore list contains a list of host IP addresses which the IDB will ignore for detection and blocking purposes. This list may be freely edited so trusted servers and hosts are not blocked. The two addresses *0.0.0.0* and *127.0.0.1* cannot be removed from the ignore list because they represent the IDB host. You may enter the IP addresses as a range, see the IP address ranges section further on for more information.

***Warning***

*A word of caution regarding automatically blocking UDP requests. Because an attacker can easily forge the source address of these requests, a host that automatically blocks UDP probes can be tricked into restricting access from legitimate services. Proper firewall rules and ignored hosts lists will significantly reduce this risk.*

## IP address ranges

IP ranges are fields that allow multiple IP addreses to be specified using a shorthand notation. Four distinct forms of range are acceptable:

1. **a.b.c.d**
2. **a.b.c.d-e**
3. **a.b.c.d-e.f.g.h**
4. **a.b.c.d/e**

The first is simply a single IP address. Thus where ever a range is permitted, a single IP address is too.

The second specifies range of IP address from **a.b.c.d** to **a.b.c.e** inclusive, i.e. you are specifying a range within a C class network or subnet. For example, *192.168.5.15-30* includes 16 IP addresses.

The third form allows the address range to span network and subnet boundaries. All addresses including and between the two specified IP addresses are included in the range. For example, *192.168.5.190-192.168.6.56* includes 123 IP addresses.

The final form allows the range to be specified to cover an entire subnet. The value of **e** specified the number of fix bits in the IP address range. Thus, **a.b.c.d/24** covers the entire C class network/subnet **a.b.c.0** and is equivalent to specifying the range as **a.b.c.0-255** (the value for **d** here can be anything as it is ignored). A range of **a.b.c.d/32** is equivalent to the single IP address **a.b.c.d**. For example, *192.168.12.150/26* is equivalent to the range *192.168.12.128-191* and it includes 64 IP addresses.

# Content filtering

The SnapGear Content Filtering system limits the types of web-based content accessed. Web-based content featuring profanity, sexually explicit or other objectionable material can be limited or blocked from the following screens.  The following figure shows content filtering:

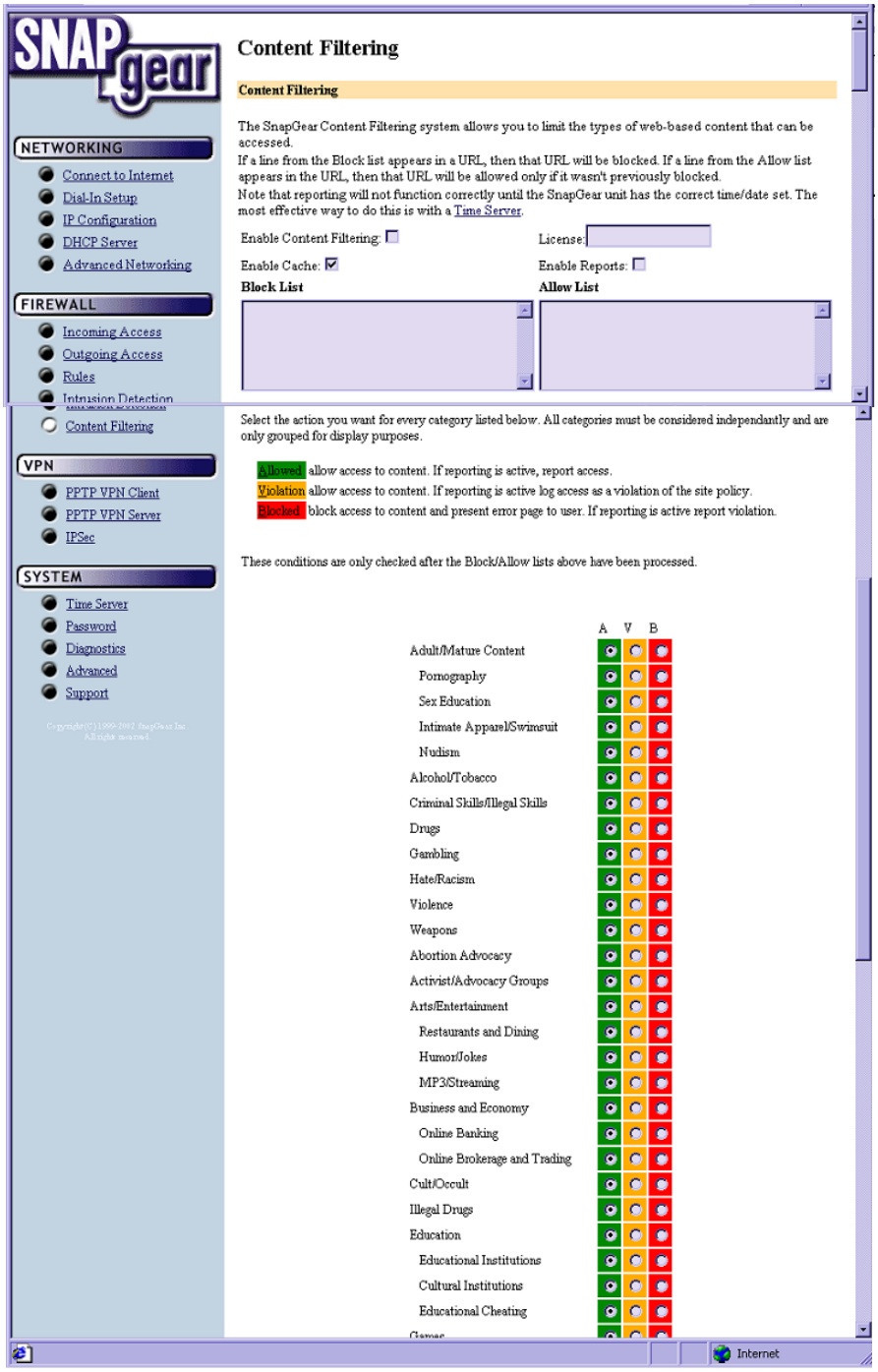

SNAPgear
Content Filtering
Content Filtering
The SnapGear Content Filtering system allows you to limit the types of web-based content that can be accessed.
If a line from the Block list appears in a URL, then that URL will be blocked. If a line from the Allow list appears in the URL, then that URL will be allowed only if it wasn't previously blocked.
Note that reporting will not function correctly until the SnapGear unit has the correct time/date set. The most effective way to do this is with a Time Server.
Enable Content Filtering:
License:
Enable Cache:
Enable Reports:
Block List
Allow List
NETWORKING
Connect to Internet
Dial-In Setup
IP Configuration
DHCP Server
Advanced Networking
FIREWALL
Incoming Access
Outgoing Access
Rules
Intrusion Detection
Content Filtering
VPN
PPTP VPN Client
PPTP VPN Server
IPSec
SYSTEM
Time Server
Password
Diagnostics
Advanced
Support
Select the action you want for every category listed below. All categories must be considered independantly and are only grouped for display purposes.
Allowed allow access to content. If reporting is active, report access.
Violation allow access to content. If reporting is active log access as a violation of the site policy.
Blocked block access to content and present error page to user. If reporting is active report violation.
These conditions are only checked after the Block/Allow lists above have been processed.
A V B
Adult/Mature Content
Pornography
Sex Education
Intimate Apparel/Swimsuit
Nudism
Alcohol/Tobacco
Criminal Skills/Illegal Skills
Drugs
Gambling
Hate/Racism
Violence
Weapons
Abortion Advocacy
Activist/Advocacy Groups
Arts/Entertainment
Restaurants and Dining
Humor/Jokes
MP3/Streaming
Business and Economy
Online Banking
Online Brokerage and Trading
Cult/Occult
Illegal Drugs
Education
Educational Institutions
Cultural Institutions
Educational Cheating
Internet

**Figure 7.8 Content filtering**

In the **Block List**, specify text that will block access to any URL containing that text. For example, if access to websites containing references to “widgets” is a violation, entering that text will block any URL containing “widgets” including **`http://www.widgets.example.com`** or **`www.test.com/widgets/index.html`**.

***Warning***

*This list only refers to the URL; it will not search and block on content.*

The **Allow List** also enables access to URLs containing the specified text.

## Filtering levels and reporting

The SnapGear **Content Filtering** screen allows you to select filtering levels based on green, yellow, and red color codes. You can select from some commonly blocked content and set the filtering levels according to your requirements.

Reporting contains the following filtering levels:

| Filtering Level | Description |
|---|---|
| Green (Allowed) | Access to content is allowed. If reporting is active, report the access. |
| Yellow (Violation) | Access to content is allowed. If reporting is active, log the access as a violation of the site policy. |
| Red (Blocked) | Access to content is blocked. Show the error page to the user. If reporting is active, log the access as a violation. |

An activity report is available by ticking the **Enable Reports** box.

***Warning***

*The correct time/date must be set on your SnapGear appliance for Reporting to work. The most effective way to do this is by using a time server.*

The filtering and reporting can only be activated after visiting the **Registration** page.

# 8. Virtual Private Networking

Virtual Private Networking (VPN) enables two or more locations to communicate securely and effectively, usually across a public network (e.g. the Internet) and has the following key traits:

- **Privacy** - no one else can see what you are communicating
- **Authentication** - you know who you are communicating with
- **Integrity** - no one else can tamper with your messages/data

Using VPN, you can access the office network securely across the Internet using Point-to-Point Tunneling Protocol (PPTP), IPSec, GRE or L2TP. If you take your portable computer on a business trip, you can dial a local number to connect to your Internet access provider and then create a second connection (called a *tunnel*) into your office network across the Internet and have the same access to your corporate network as if you were connected directly from your office. Similarly, telecommuters can also set up a VPN tunnel over their cable modem or DSL links to their local ISP.

VPN technology can also be deployed as a low cost way of securely linking two or more networks, such as a headquarters LAN to the branch office(s). IPSec is generally the most suitable choice in this scenario.

With the SnapGear appliance you can establish a VPN tunnel over the Internet using either PPTP, IPSec, GRE or L2TP. IPSec provides the best security; however PPTP is the preferred protocol for integrating with existing Microsoft infrastructure. GRE and L2TP VPNs will generally be used for specialized purposes only. The SnapGear appliance provides a PPTP server to enable remote Windows clients to securely access your office network. Using the SnapGear appliance's PPTP client or IPSec you can also connect your office network to one or more remote networks.

This chapter details how to configure the PPTP server and client and how to configure a remote client to connect, how to establish an IPSec tunnel, and also provides an overview of GRE and L2TP VPN tunneling.

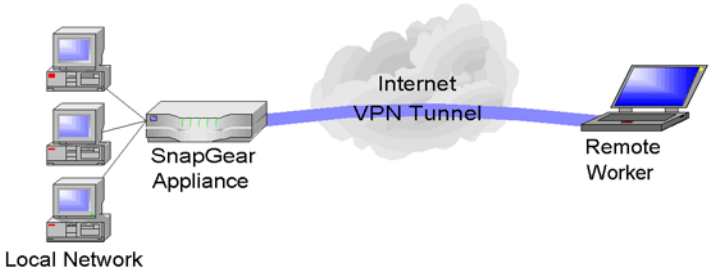



**Figure 8.1 VPN tunneling using the PPTP server**

# PPTP client setup

The SnapGear PPTP client enables the SnapGear appliance to establish a VPN to a remote network running a PPTP server (usually a Microsoft Windows server).

To set up a SnapGear PPTP VPN Client, select **PPTP VPN Client** from the **VPN** menu and create a new VPN connection by entering:

- A descriptive **name** for the VPN connection. This may describe the purpose for the connection.
- The remote PPTP **server IP address** to connect to.
- A **username** and **password** to use when logging in to the remote VPN. You may need to obtain this information from the system administrator of the remote PPTP server and,
- Optionally, the remote network's **netmask**. This is used to determine which packets should go the remote network.
- Click **Add**.

***Warning***

*If you are using Windows 98, you must ensure that Dial Up Networking has been upgraded to version 1.4 otherwise you will be unable to use MS-CHAPv2 authentication (the recommended method).*

If the remote VPN is already up and running, check **Start Now** to establish the connection immediately as shown in the following figure:

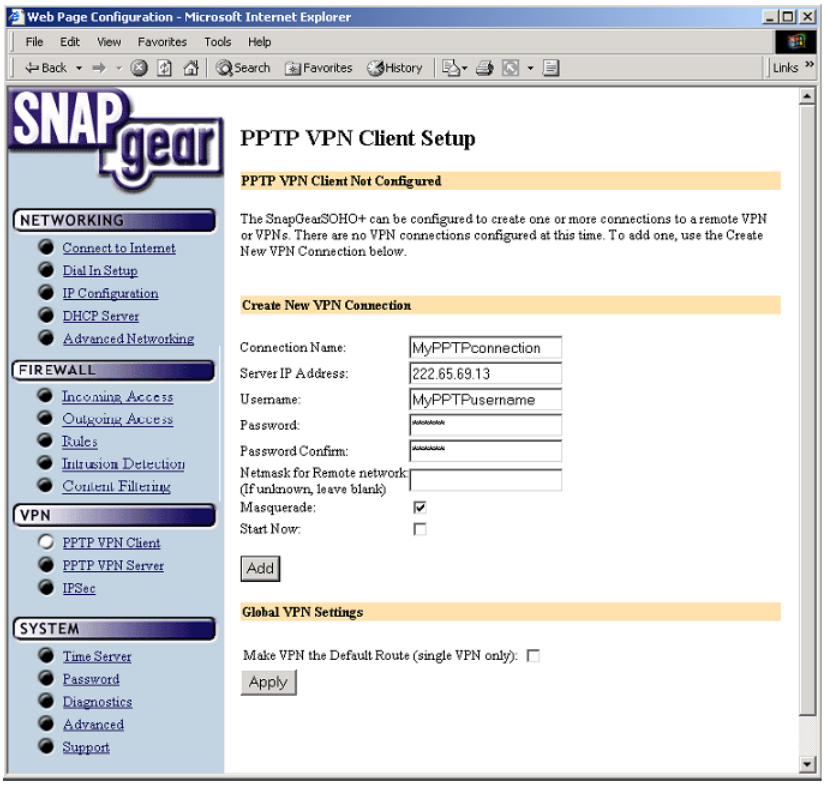



**Figure 8.2 PPTP client configuration**

The SnapGear appliance supports multiple VPN client connections. Additional connections can be added by following these steps. To set a VPN connection as the default route for all network traffic, check the **Make VPN the Default Route** checkbox and click **Apply**. This option is only available when the SnapGear appliance is configured with a single VPN connection only.

After adding a new VPN, two new tables are displayed in the **PPTP VPN Client** menu. **VPN Connection Status** provides information about the **State** of the VPN (i.e. enabled or disabled) and the **Status** of the connection (i.e. up or down).

The **VPN Configuration** table provides the ability to enable/disable the VPN, edit the VPN configuration, delete the VPN entry and edit the advanced routing information.

# PPTP server setup

The SnapGear appliance includes a PPTP Server, a virtual private network server that supports up to forty simultaneous VPN tunnels (depending on your SnapGear appliance model). The SnapGear PPTP Server allows remote Windows clients to securely connect to the local network.

To setup a VPN connection:

- Enable and configure the PPTP VPN server.
- Set up VPN user accounts on the SnapGear appliance and enable the appropriate authentication security.
- Configure the VPN clients at the remote sites. The client does not require special software. The SnapGear PPTP Server supports the standard PPTP client software included with Windows 95/98, Windows ME, Windows XP, WinNT and Windows 2000. The VPN connection is simple to configure using the standard Dial-Up Networking software. The SnapGear PPTP Server is also compatible with Unix PPTP client software.
- Connect the remote VPN client.

The following sections provide additional detailed instructions.

## Enable and configure the PPTP VPN server

The following figure shows the PPTP server setup:

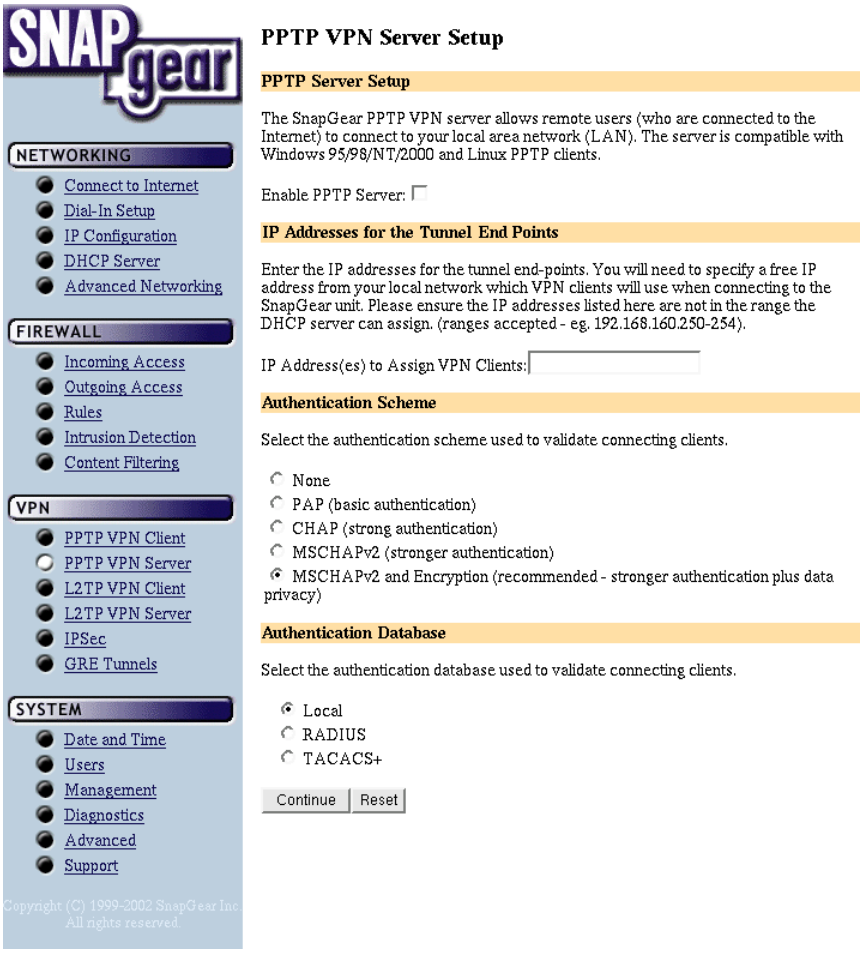

SNAPgear
NETWORKING
Connect to Internet
Dial-In Setup
IP Configuration
DHCP Server
Advanced Networking
FIREWALL
Incoming Access
Outgoing Access
Rules
Intrusion Detection
Content Filtering
VPN
PPTP VPN Client
PPTP VPN Server
L2TP VPN Client
L2TP VPN Server
IPSec
GRE Tunnels
SYSTEM
Date and Time
Users
Management
Diagnostics
Advanced
Support
Copyright (C) 1999-2002 SnapGear Inc.
All rights reserved.
PPTP VPN Server Setup
PPTP Server Setup
The SnapGear PPTP VPN server allows remote users (who are connected to the Internet) to connect to your local area network (LAN). The server is compatible with Windows 95/98/NT/2000 and Linux PPTP clients.
Enable PPTP Server:
IP Addresses for the Tunnel End Points
Enter the IP addresses for the tunnel end-points. You will need to specify a free IP address from your local network which VPN clients will use when connecting to the SnapGear unit. Please ensure the IP addresses listed here are not in the range the DHCP server can assign. (ranges accepted - eg. 192.168.160.250-254).
IP Address(es) to Assign VPN Clients:
Authentication Scheme
Select the authentication scheme used to validate connecting clients.
None
PAP (basic authentication)
CHAP (strong authentication)
MSCHAPv2 (stronger authentication)
MSCHAPv2 and Encryption (recommended - stronger authentication plus data privacy)
Authentication Database
Select the authentication database used to validate connecting clients.
Local
RADIUS
TACACS+
Continue
Reset

**Figure 8.3 PPTP server setup**

To enable and configure your SnapGear appliance's VPN server, select **PPTP VPN Server** from the **VPN** menu on the *SnapGear Management Console* web administration pages.

The following table describes the fields in the VPN Setup screen and the options available when enabling and configuring VPN access.

| Field | Description |
|---|---|
| Enable PPTP Server | Check this box to enable PPTP connections to be established to your SnapGear appliance. |
| IP Addresses for the Tunnel End Points | Enter the IP addresses for the tunnel end-points. You need to specify a free IP address on your local network that each VPN client will use when connecting to the SnapGear appliance. Please ensure that the IP addresses listed here are not in the range the DHCP server can assign. Ranges are accepted; for example 192.168.160.250-254. |
| Authentication Scheme | PPTP provides an authenticated communication tunnel between a client and a gateway by using a user ID and password. The authentication scheme is the method the SnapGear appliance uses to challenge users wanting to establish a PPTP connection to the network. The remote client must be set up to use the selected authentication scheme.<br>• **MSCHAPv2** is the most secure. *SnapGear recommends the use of **MSCHAPv2 plus data encryption** as this keeps your data private as well as providing secure authentication.*<br>• **CHAP** is less secure<br>• **PAP** (although more common) is even less secure.<br>• **None** means that no username/password authentication is required. |
| Authentication Database | The authentication database is used to verify the username and password received from the dial-in client.<br>• **Local** means the PPTP user accounts created on the SnapGear appliance. You will need to created user accounts as described below. This can be used with any authentication scheme.<br>• **RADIUS** means an external RADIUS server. You will be prompted to enter the server IP address and password. This can be used with any authentication scheme, provided that the RADIUS server also supports it.<br>• **TACACS+** means an external TACACS+ server. You will be prompted to enter the server IP address and password. This can only be used with the **PAP** authentication scheme. |

## Configuring user accounts for VPN server

After setting up the VPN server, select **Continue** and to show the *PPTP VPN Server Accounts* screen as shown in the following figure:

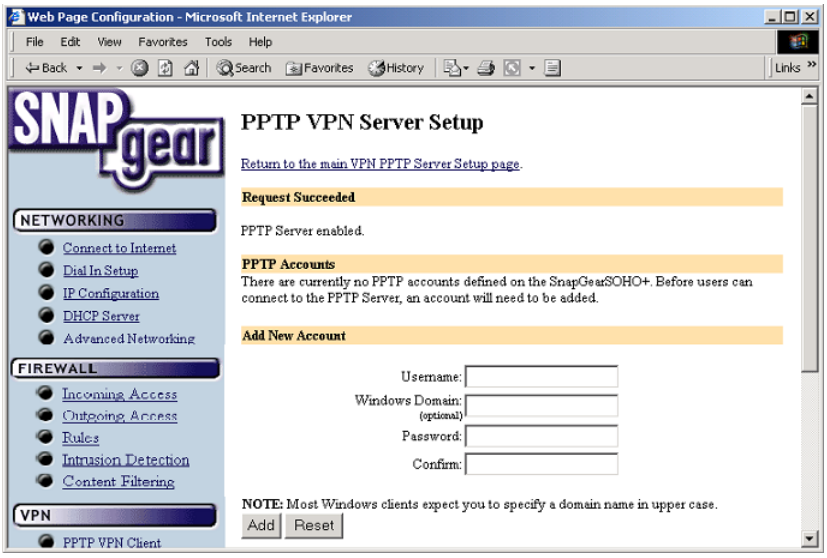



**Figure 8.4 PPTP VPN server accounts screen**

Before remote users can set up a VPN tunnel to the SnapGear appliance PPTP server, they must have a user accounts set up. The field options in the **Add New Account** are detailed in the following table.

| Field | Description |
|---|---|
| Username | Username for VPN authentication only. The name selected is case-sensitive (e.g. *Jimsmith* is different to *jimsmith*). Username can be the same as, or different to, the name set for dial-in access. |
| Windows Domain | Most Windows clients expect you to specify a domain name in upper case. This field is optional. |
| Password | Enter the password for the remote VPN user. |
| Confirm | Re-enter the password to confirm. |

As new VPN user accounts are added, they are displayed on the updated *Account List*.

To modify the password of an existing account, **Select** the account in the **Account List** and then enter **New Password** and **Confirm** in the **Delete or Change Password for the Selected Account** field.

To delete an existing account, **Select** the account in the **Account List** and then check **Delete** in the **Delete or Change Password for the Selected Account** field.

If a requested change to a user account is successful, the **PPTP VPN Setup** screen is shown with the change noted. An error is displayed if the change request is unsuccessful.

## Configuring the remote VPN client

After setting up the SnapGear PPTP VPN server, the remote VPN clients can be configured to securely access the local network. You need to enter the VPN client username and password that your remote users will use to access the SnapGear PPTP VPN from the remote site.

The names may or may not be the same as your normal network username and password, and should be different from the username and password used by your remote users use to access their local ISP.

The following figure shows the VPN PPTP IP address:

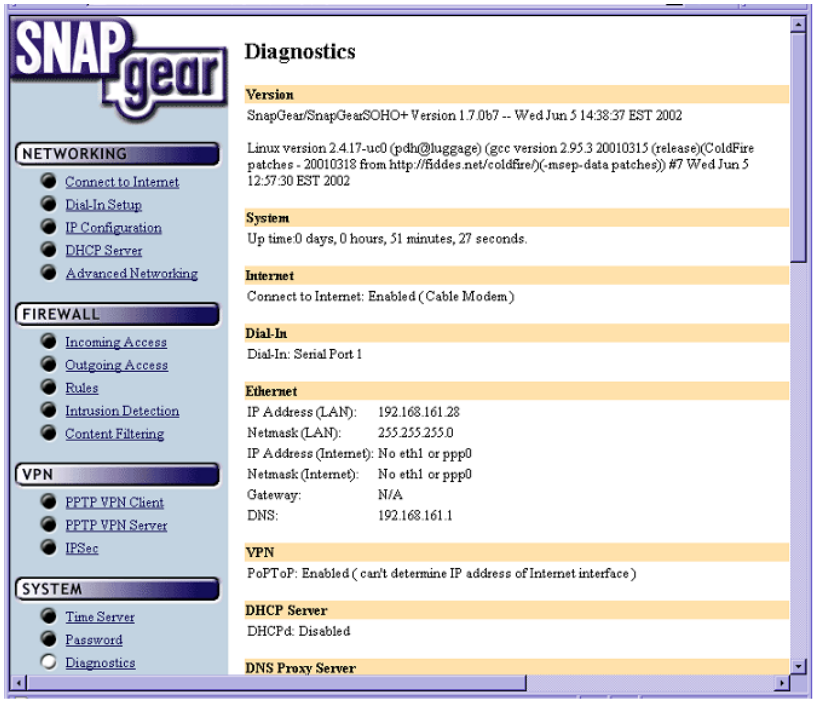



**Figure 8.5 VPN PPTP IP address**

Obtain the current IP address of the SnapGear appliance PPTP server. This address may change if your office network has an external DHCP server (i.e. your ISP dynamically assigns your an IP address).

To determine the current SnapGear appliance's PPTP server IP address, select **Diagnostics** from the **System** menu in the main menu bar. The IP address is displayed in the **VPN** field. Your remote users must know this **PPTP IP address** to setup a VPN tunnel to the SnapGear appliance.

Check that the remote PC has a modem installed and that you have a local ISP account, (i.e. ISP phone number(s), username and password to log in to the ISP). Although users are often connected to the Internet using a dial-out modem, VPN connection can also be set up using a cable modem, ADSL, ISDN or other Internet link.

Ensure that both the VPN and Dial Up Networking (DUN) software is installed on the remote PC. If necessary, install the *Microsoft DUN update* (available on the SnapGear Installation CD) and *VPN Client update.*

To create a VPN connection across the Internet, you must set up two networking connections. One connection is for the Internet access provider, and the other connection is for the VPN tunnel to your office network. Verify that a networking connection is established for the link to your local ISP.

Set up a new connection for the VPN connection. Your SnapGear appliance's PPTP server will operate with the standard Windows PPTP clients in all versions of Windows.

The following sections provide details for client setup in Windows 95/98, Windows NT, and Windows 2000. Setup instructions for Windows ME and Windows XP can be deduced from this information and the Microsoft Windows documentation.

## Windows 95 and Windows 98

From the Dial-Up Networking folder, double-click **Make New Connection**. Type **SnapGear appliance** or a similar descriptive name for your new VPN connection.

From the **Select a device** drop-down menu, select the **Microsoft VPN Adapter** and click **Next**. Enter the PPTP IP address of the SnapGear appliance VPN server in the **VPN Server** field. This may change if your ISP uses dynamic IP assignment. Click **OK** and then click **Finish**.

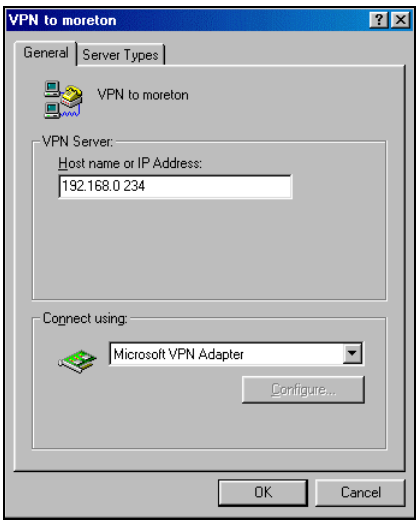



**Figure 8.6 VPN client setup**

Right-click the new icon and select **Properties**.

Select the **Server Types** tab and check the **Log on to network**, **Enable software compression**, and **Require encrypted password** checkboxes. Leave the other ***Advanced Options*** unchecked.

Select the **TCP/IP** network protocols from the **Allowed network protocols** list.

***Warning***

*Do not select NetBEUI or IPX. If an unsupported protocol is selected, an error message is returned.*

Click ***TCP/IP Settings***. Confirm that the **Server Assigned IP Address**, **Server Assigned Name Server Address**, **Use IP Header Compression** and **Use Default Gateway on Remote Network** are all selected and click **OK**.

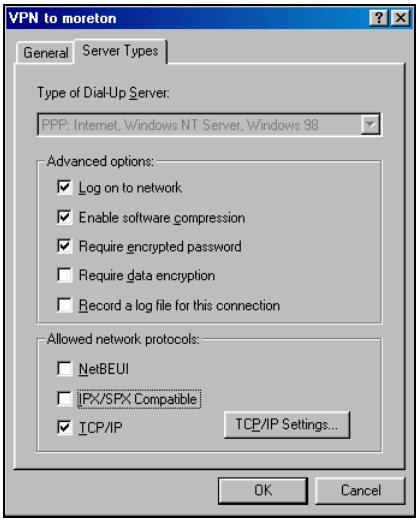



**Figure 8.7 VPN client server settings**

Your VPN client is now set up correctly.

Windows NT

From the **Dial-Up Networking** dialog, click **New** and select the **Basic** tab.

In the **Entry name** field, enter **SnapGear appliance** or a similar descriptive name and click **Next**.

Enter the SnapGear appliance's *PPTP IP address* into the **Phone Number** field.

***Warning***

*Note that this IP address may change if your ISP uses dynamic IP assignment.*

In the **Dial Using** dialog box, select **RASSPPTPM (VPN1)** and click **Next**.

Click **More** and select **Edit entry** then **Modem properties** from the menu.

Select the **Server** tab.

Select **TCP/IP** only.

***Warning***

*Do not select NetBEUI or IPX. If an unsupported protocol is selected, an error message is returned.*

Select the **Security** tab and select **Accept only Microsoft encrypted authentication**. Click **OK**.

Your VPN client is now set up correctly.

## Windows 2000

To set up VPN access, first setup a Dial Up Networking account to access the Internet. Once you have done this, you are ready to begin.

The first thing you need to do is log in as Administrator on your PC. After logging in, from the **Start** menu, select **Settings** and then **Network and Dial-up Connections** as shown in the following figure:

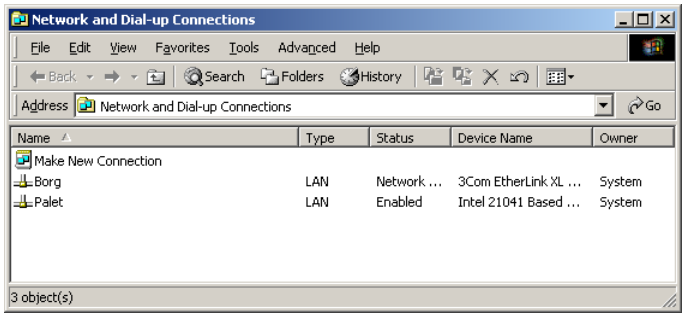

Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go
Name Type Status Device Name Owner
Make New Connection
Borg LAN Network ... 3Com EtherLink XL ... System
Palet LAN Enabled Intel 21041 Based ... System
3 object(s)

**Figure 8.8 Network and dial-up connections**

To set up your VPN account, double-click **Make New Connection** and then click **Next** to show the **Network Connection Type** window:

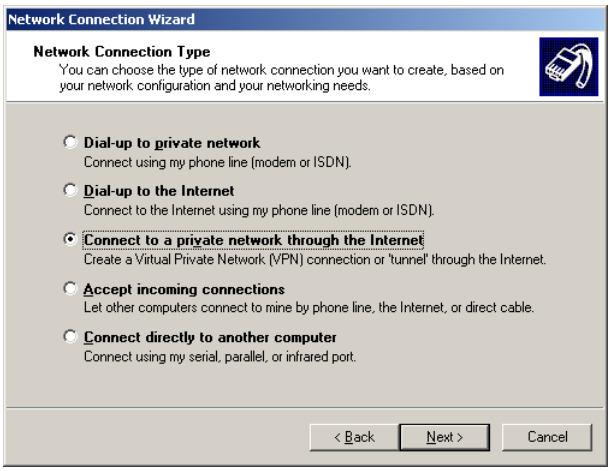

Network Connection Wizard
Network Connection Type
You can choose the type of network connection you want to create, based on your network configuration and your networking needs.
Dial-up to private network
Connect using my phone line (modem or ISDN).
Dial-up to the Internet
Connect to the Internet using my phone line (modem or ISDN).
Connect to a private network through the Internet
Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.
Accept incoming connections
Let other computers connect to mine by phone line, the Internet, or direct cable.
Connect directly to another computer
Connect using my serial, parallel, or infrared port.
< Back
Next >
Cancel

**Figure 8.9 Network connection type**

Select **Connect to a private network through the Internet** and click **Next**.

This displays the **Destination Address** window:

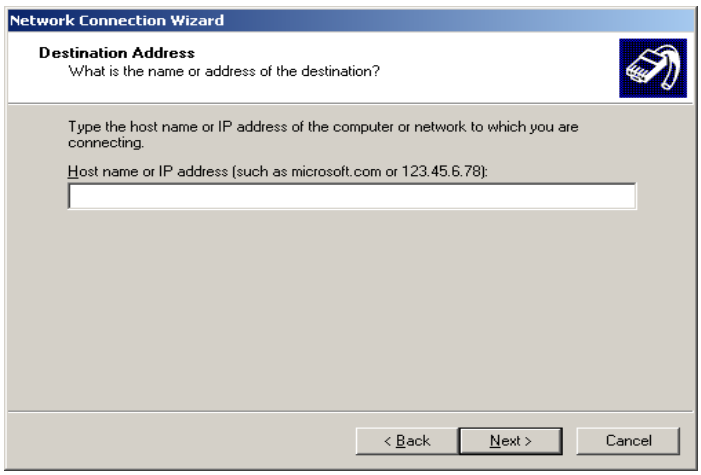

Network Connection Wizard
Destination Address
What is the name or address of the destination?
Type the host name or IP address of the computer or network to which you are connecting.
Host name or IP address (such as microsoft.com or 123.45.6.78):
< Back
Next >
Cancel

**Figure 8.10 Destination address**

Enter the SnapGear PPTP server's IP address and click **Next**. Select the **Connection Availability** you require on the next window and click **Next** to display the final window:

Network Connection Wizard
Completing the Network Connection Wizard
Type the name you want to use for this connection:
Virtual Private Connection
To create this connection and save it in the Network and Dial-up Connections folder, click Finish.
To edit this connection in the Network and Dial-up Connections folder, select it, click File, and then click Properties.
Add a shortcut to my desktop
< Back
Finish
Cancel

**Figure 8.11 Completing the network connection wizard**

Enter an appropriate name for your connection and click **Finish**.

Your VPN client is now set up correctly.

## Connecting the remote VPN client

Firstly, connect to the Internet using the network connection to your ISP.

After authenticating the connection to your ISP, select the connection for the SnapGear appliance VPN.

For *Windows 95/98/2000*, enter the username and password allocated by your SnapGear appliance's VPN administrator and click **Connect**.

For *Windows NT*, click **Dial** and enter the username and password *allocated* by your SnapGear appliance's VPN administrator.

After you are authenticated to the network, you can check your e-mail, use the office printer, access shared files and browse the network as if you were physically on the LAN.

To disconnect the VPN tunnel connection to the remote SnapGear appliance:

- On the desktop, double-click **My Computer** then **Dial-Up Networking** and select the phonebook entry for the SnapGear appliance VPN.
- For *Windows 95/98/2000*, click the **Disconnect** button
- For *Windows NT*, click the **Hang up** button

You can then disconnect from the Internet.

# IPSec setup

## SnapGear to SnapGear

There are many possible configurations in creating an IPSec tunnel. The most common and simplest will be described in this section. Additional options will also be explained throughout this example, should it become necessary to configure the tunnel with those settings. For most applications to connect two offices together, a network similar to the following will be used.

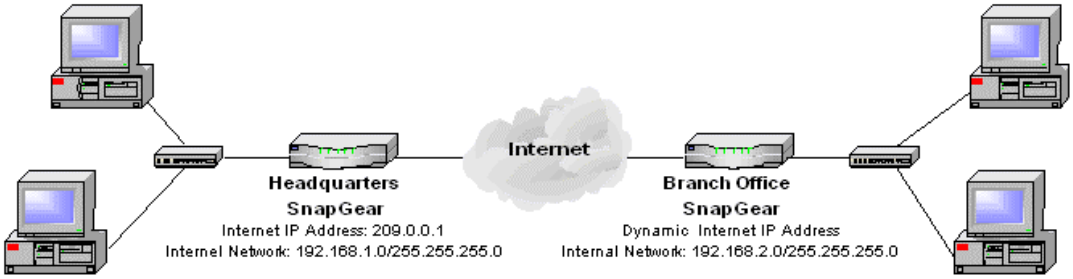



**Figure 8.12 IPSec tunnel network diagram**

To combine the Headquarters and Branch Office networks together, an IPSec tunnel must be configured on both SnapGear appliances.

# Configuring the branch office SnapGear appliance

## Enabling IPSec

Click the IPSec link on the left side of the *SnapGear Management Console* web administration pages. A window similar to the following will be displayed.

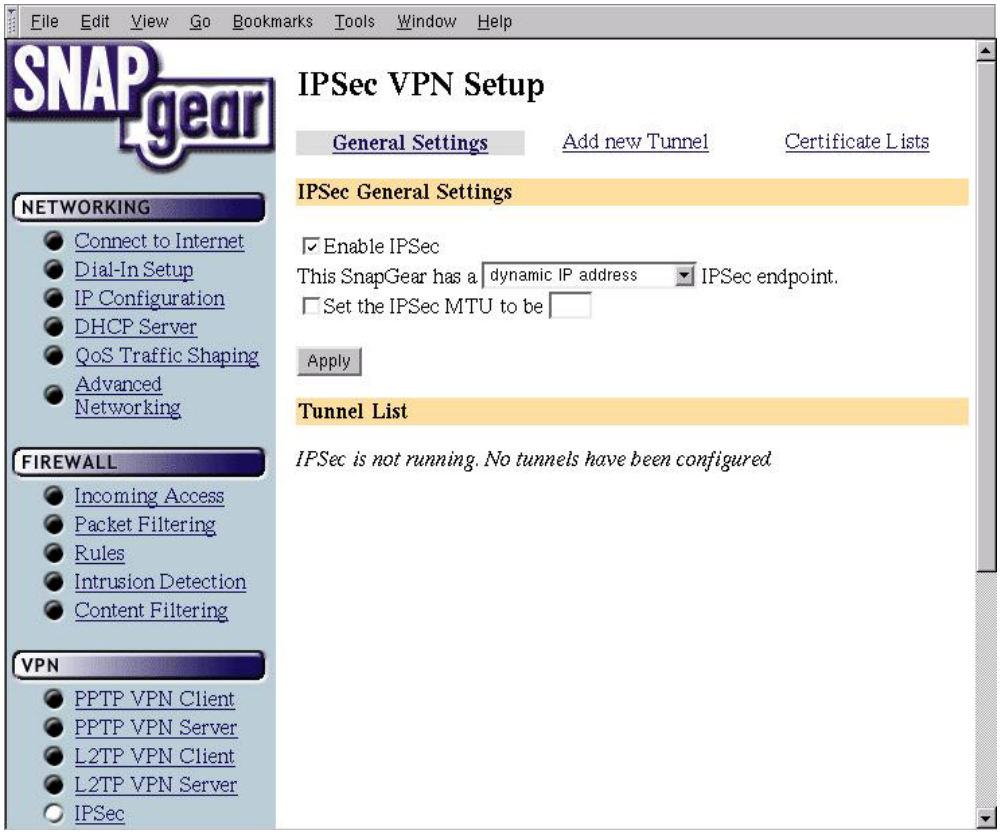



**Figure 8.13 Enabling IPSec**

Check the **Enable IPSec** checkbox.

Select the type of IPSec endpoint the SnapGear appliance has on its Internet interface. The SnapGear can either have a **static IP**, **dynamic IP** or **DNS hostname address**. If a dynamic DNS service is to be used or there is a DNS hostname that resolves to the IP address on the Internet interface, then the DNS hostname address option should be selected. In this example, select **dynamic IP address**.

The Maximum Transmission Unit (**MTU**) of the IPSec interface can be configured by checking the **Set the IPSec MTU to be** checkbox and filling in the desired MTU value. For most applications this need not be configured, however if it is set, the MTU value should be between 1400 and 1500. In this example leave the checkbox unchecked. Click the **Apply** button to save the changes.

***Warning***

*It may be necessary to reduce the MTU of the IPSec interface if large packets of data are not being transmitted.*

## Configure a Tunnel to Connect to the Headquarters Office

To create an IPSec tunnel, click the **IPSec** link on the left side of the *SnapGear Management Console* web administration pages and then click the **Add New Tunnel** tab at the top of the window. A window similar to the following will be displayed.

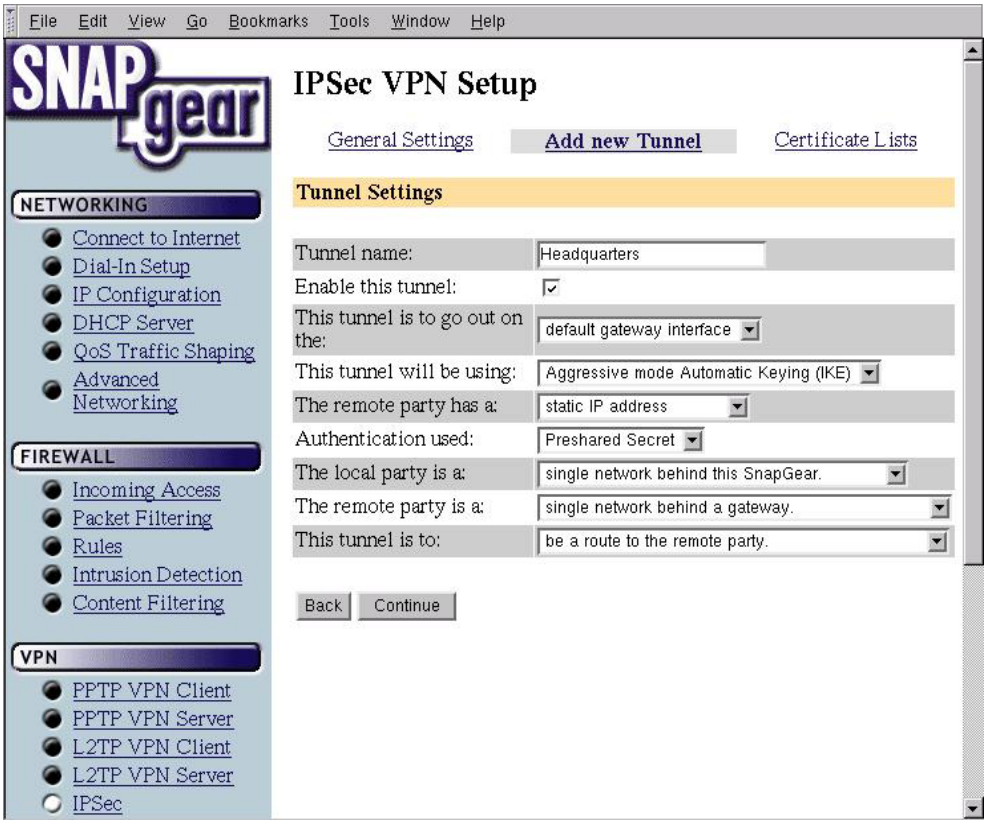



**Figure 8.14 Add new tunnel**

## Tunnel Settings Page

Fill in the **Tunnel name** field with an apt description for the tunnel. The name must not contain spaces or start with a number. In this example, enter *Headquarters*.

Leave the **Enable this tunnel** checkbox checked.

Select the Internet interface the IPSec tunnel is to go out on. The options will depend on what is currently configured on the SnapGear appliance. For the vast majority of setups, this will be the **default gateway interface** to the Internet. In this example, select the **default gateway interface** option.

***Note***

*You may want to select an interface other than the default gateway when you have configured aliased Internet interfaces and require the IPSec tunnel to run on an interface other than the default gateway.*

Select the type of keying the tunnel will use. The SnapGear appliance supports the following types of keying:

- **Main mode with Automatic Keying (IKE)** automatically exchanges encryption and authentication keys and protects the identities of the parties attempting to establish the tunnel.

- **Aggressive mode with Automatic Keying (IKE)** automatically exchanges encryption and authentication keys and uses less messages in the exchange when compared to Main mode. Aggressive mode is typically used to allow parties that are configured with a dynamic IP address and a preshared secret to connect or if the SnapGear appliance or the remote party is behind a NAT device.

- **Manual Keying** requires the encryption and authentication keys to be specified.

In this example, select the **Aggressive mode with Automatic Keying** option.

Select the type of IPSec endpoint the remote party has. The remote endpoint can have a **static IP address**, **dynamic IP address** or a **DNS hostname address**. In this example, select the **static IP address** option.

Select the type of authentication the tunnel will use. The SnapGear appliance supports the following types of authentication:

- **Preshared Secret** is a common secret (passphrase) that is shared between the SnapGear appliance and the remote party.

- **RSA Digital Signatures** uses a public/private RSA key pair for authentication. The SnapGear appliance can generate these key pairs. The public keys need to be exchanged between the SnapGear appliance and the remote party in order to configure the tunnel.

- **x.509 Certificates** are used to authenticate the remote party against a Certificate Authority's (CA) certificate. The CA certificate must have signed the local certificates that are used for tunnel authentication. Certificates need to be uploaded to the SnapGear appliance before a tunnel can be configured to use them (see *Certificate Management*).

- **Manual Keys** establishes the tunnel using predetermined encryption and authentication keys.

In this example, select the **Preshared Secret** option.

Select the type of private network that is behind the SnapGear appliance. The following types of networks are supported:

- **Single network** is selected when a single subnet resides behind the SnapGear appliance that the remote party will have access to.

- **Multiple networks** is selected when multiple subnets reside behind the SnapGear appliance that the remote party will have access to.

- **Masqueraded network** is selected when all traffic behind the SnapGear appliance is seen as originating from its Internet IP address by the remote party. The remote party will not have any access to the network behind the SnapGear appliance.

In this example, select the **single network behind this SnapGear** option.

Select whether the remote party is a **single host** or whether it is a gateway that has a **single network** or has **multiple networks** behind it. In this example, select the **single network behind a gateway** option.

Select in which way the tunnel should be utilized to route traffic. The SnapGear can support following types of routing:

- **Be a route to the remote party** is selected when the tunnel sets up a route to the remote party's subnet(s).

- **Be this SnapGear's default gateway for all traffic** is selected when the tunnel will be the default gateway for all traffic to the remote party.

- **Be the remote party's default gateway for all traffic** is selected when the tunnel will be the default gateway for all traffic from the remote party.

In this example, select the **be a route to the remote party** option.

Click the **Continue** button to configure the **Local Endpoint Settings**.

## Local Endpoint Settings

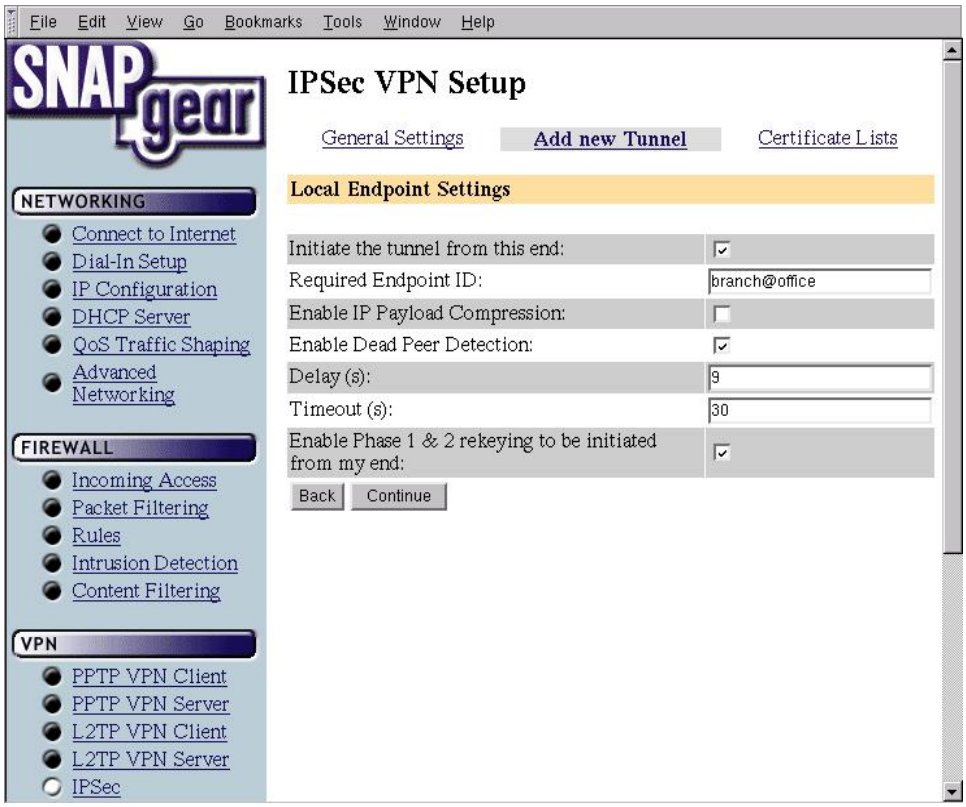



**Figure 8.15 Local Endpoint Settings**

Leave the **Initiate the tunnel from this end** checkbox checked.

***Note***

*This option will not be available when the SnapGear appliance has a static IP address and the remote party has a dynamic IP address.*

Enter the **Required Endpoint ID** of the SnapGear. This ID is used to authenticate the SnapGear appliance to the remote party. It is required because the SnapGear appliance in this example has a dynamic IP address. This field will also be required if RSA Digital Signatures are used for authentication.

It becomes optional if the SnapGear appliance has a static IP address and is using Preshared Secrets for authentication. If it is optional and the field is left blank, the **Endpoint ID** defaults to the static IP address. If the remote party is a SnapGear appliance, the ID must have the form *abcd*@*efgh*. If the remote party is not a SnapGear appliance, refer the interoperability documents on the SnapGear knowledge base web site (**`http://www.snapgear.com/knowledgebase.html`**) to determine what form it must take. In this example, enter: **branch@office**

Leave the **Enable IP Payload Compression** checkbox unchecked. If compression is selected, *IPComp* compression is applied before encryption.

Check the **Enable Dead Peer Detection** checkbox. This allows the tunnel to be restarted if the remote party stops responding. This option is only used if the remote party supports Dead Peer Detection. It operates by sending notifications and waiting for acknowledgements.

Enter the **Delay** and **Timeout** values for Dead Peer Detection. The default times for the delay and timeout options are 9 and 30 seconds respectively. This means that a Dead Peer Detection notification will be sent every 9 seconds (**Delay**) and if no response is received in 30 seconds (**Timeout**) then the SnapGear appliance will attempt to restart the tunnel. In this example, leave the delay and timeout as their default values.

Leave the **Enable Phase 1 & 2 rekeying to be initiated from my end** checkbox checked. This enables automatic renegotiation of the tunnel when the keys are about to expire.

Click the **Continue** button to configure the **Remote Endpoint Settings**.

## Other Options

The following options will become available on this page depending on what has been configured previously:

- **The next IP address on the interface the tunnel is to go on** field is the next gateway IP address or *nexthop* along the previously selected IPSec interface. This field will become available if an interface other than the default gateway was selected for the tunnel to go out on.

- **SPI Number** field is the *Security Parameters Index*. It is a hexadecimal value and must be unique. It is used to establish and uniquely identify the tunnel. The SPI is used to determine which key is used to encrypt and decrypt the packets. It must be of the form 0x*hex*, where *hex* is one or more hexadecimal digits and be in the range of *0x100-0xfff*. This field appears when **Manual Keying** has been selected.

- **Authentication Key** field is the *ESP Authentication Key*. It must be of the form 0x*hex*, where *hex* is one or more hexadecimal digits. The *hex* part must be exactly 32 characters long when using MD5 or 40 characters long when using SHA1 (excluding any underscore characters). This field appears when **Manual Keying** has been selected.

- **Encryption Key** field is the *ESP Encryption Key*. It must be of the form 0x*hex*, where *hex* is one or more hexadecimal digits. The *hex* part must be exactly 16 characters long when using DES or 48 characters long when using 3DES (excluding any underscore characters). This field appears when **Manual Keying** has been selected.

- **Cipher and Hash** pull down menu contains the ESP encryption/authentication algorithms that can be used for the tunnel. The option selected must correspond to the encryption and authentication keys used. This pull down menu appears when **Manual Keying** has been selected. The options include the following:

    - **3des-md5-96** uses the encryption transform following the Triple-DES standard in Cipher-Block-Chaining mode with authentication provided by HMAC and MD5 (96-bit authenticator). It uses a 192-bit 3DES encryption key and a 128-bit HMAC-MD5 authentication key.

    - **3des-sha1-96** uses the encryption transform following the Triple-DES standard in Cipher-Block-Chaining mode with authentication provided by HMAC and SHA1 (96-bit authenticator). It uses a 192-bit 3DES encryption key and a 160-bit HMAC-SHA1 authentication key.

    - **des-md5-96** uses the encryption transform following the DES standard in Cipher-Block-Chaining mode with authentication provided by HMAC and MD5 (96-bit authenticator). It uses a 56-bit 3DES encryption key and a 128-bit HMAC-MD5 authentication key.

- **des-sha1-96** uses the encryption transform following the DES standard in Cipher-Block-Chaining mode with authentication provided by HMAC and SHA1 (96-bit authenticator). It uses a 56-bit DES encryption key and a 160-bit HMAC-SHA1 authentication key.

- **Local Network** field is the network behind the local SnapGear appliance. This field appears when **Manual Keying** has been selected.

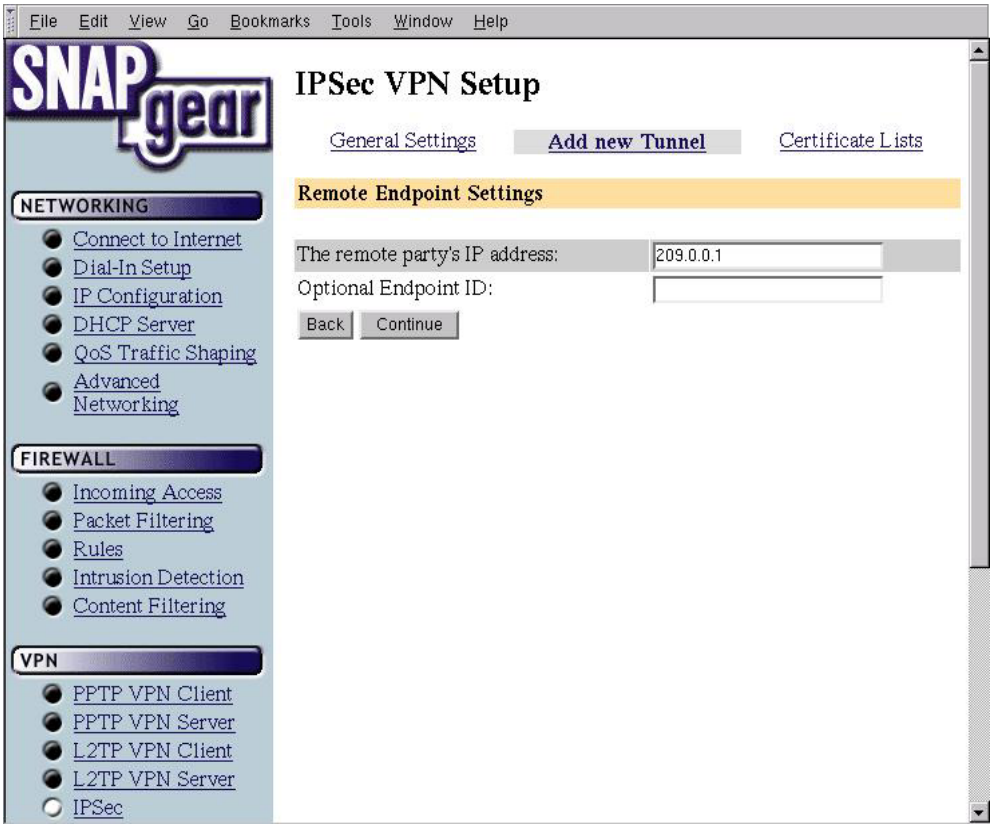



**Figure 8.16 Remote Endpoint Settings**

Enter the Internet IP address of the remote party in **The remote party's IP address** field. In this example, enter: **209.0.01**

The **Endpoint ID** is used to authenticate the remote party to the SnapGear appliance. The remote party's ID is optional if it has a static IP address and uses Preshared Secrets for authentication. It becomes a required field if the remote party has a dynamic IP or DNS hostname address or if RSA Digital Key Signatures are used for authentication. It is optional in this example, because the remote party has a static IP address. If the remote party is a SnapGear appliance, it must have the form *abcd@efgh*. If the remote party is not a SnapGear appliance, refer the interoperability documents on the SnapGear knowledge base web site (**http://www.snapgear.com/knowledgebase.html**) to determine what form it must take. In this example leave the field blank.

Click the **Continue** button to configure the **Phase 1 Settings**.

## Other Options

The following options will become available on this page depending on what has been configured previously:

- **The remote party's DNS hostname address** field is the DNS hostname address of the Internet interface of the remote party. This option will become available if the remote party has been configured to have a DNS hostname address.

- **Distinguished Name** field is the list of attribute/value pairs contained in the certificate. The list of attributes supported are as follows:

| | |
|---|---|
| **C** | Country |
| **ST** | State or province |
| **L** | Locality or town |
| **O** | Organization |
| **OU** | Organizational Unit |
| **CN** | Common Name |
| **N** | Name |
| **G** | Given name |
| **S** | Surname |
| **I** | Initials |

| | |
|---|---|
| **T** | Personal title |
| **E** | E-mail |
| **Email** | E-mail |
| **SN** | Serial number |
| **D** | Description |
| **TCGID** | [Siemens] Trust Center Global ID |

The attribute/value pairs must be of the form *attribute*=*value* and be separated by commas. For example : C=US, ST=Illinois, L=Chicago, O=SnapGear, OU=Sales, CN=SME550. It must match exactly the **Distinguished Name** of the remote party's local certificate to successfully authenticate the tunnel. This field appears when **x.509 Certificates** has been selected.

- **Generate an RSA key of** pull down menu allows the length of the SnapGear appliance generated RSA public/private key pair to be specified. The options include 512, 1024, 1536 and 2048 bits. The greater the key pair length, the longer the time required to generate the keys. It may take up to 20 minutes for a 2048 bit RSA key to be generated. This option appears when RSA Digital Key Signatures has been selected.

- **SPI Number** field is the *Security Parameters Index*. However, this applies to the remote party. It is a hexadecimal value and must be unique. It is used to establish and uniquely identify the tunnel. It must be of the form 0x*hex*, where *hex* is one or more hexadecimal digits and be in the range of *0x100-0xfff*. This field appears when **Manual Keying** has been selected.

- **Authentication Key** field is the ESP Authentication Key. However, this applies to the remote party. It must be of the form 0x*hex*, where *hex* is one or more hexadecimal digits. The *hex* part must be exactly 32 characters long when using MD5 or 40 characters long when using SHA1 (excluding any underscore characters). It must use the same hash as the SnapGear appliance's authentication key. This field appears when **Manual Keying** has been selected.

- **Encryption Key** field is the ESP Encryption Key. However, this applies to the remote party. It must be of the form 0x*hex*, where *hex* is one or more hexadecimal digits. The *hex* part must be exactly 16 characters long when using DES or 48 characters long when using 3DES (excluding any underscore characters). It must use the same cipher as the SnapGear appliance's encryption key. This field appears when **Manual Keying** has been selected.

- **Remote Network** is the network behind the remote party. This field appears when **Manual Keying** has been selected.

Phase 1 Settings

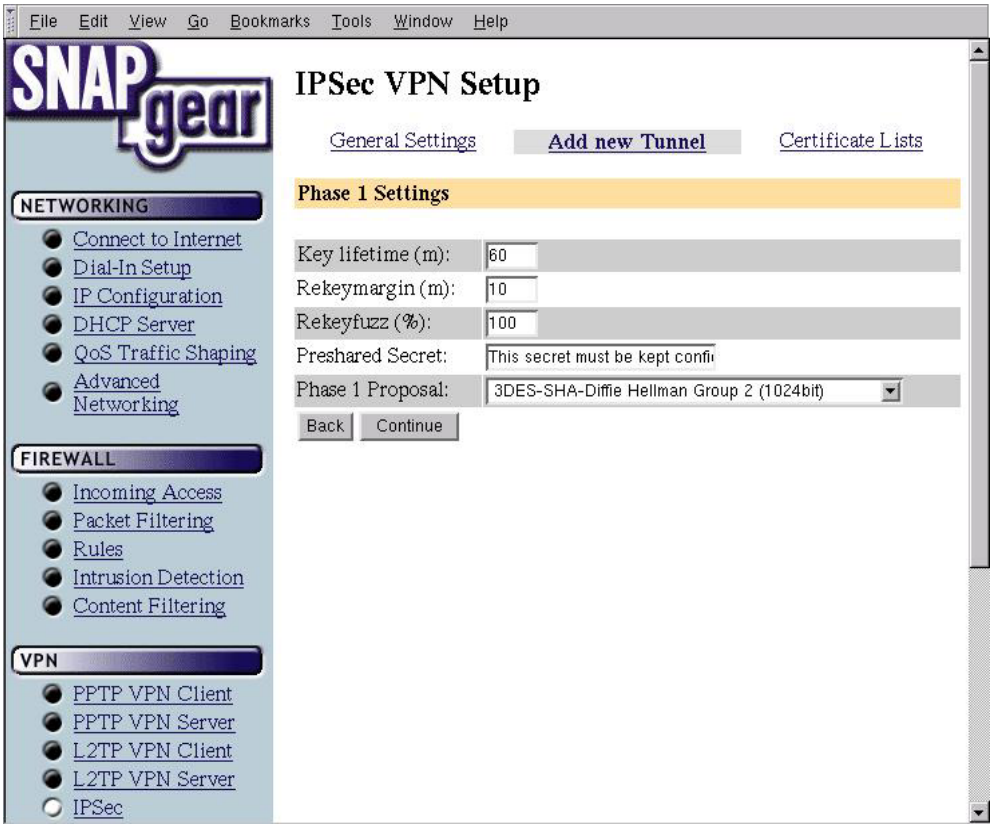



**Figure 8.17 Phase 1 Settings**

Set the length of time before Phase 1 is renegotiated in the **Key lifetime (m)** field. The length may vary between 1 and 1440 minutes. Shorter values offer higher security at the expense of the computational overhead required to calculate new keys. For most applications 60 minutes is recommended. In this example, leave the **Key Lifetime** as the default value of 60 minutes.

A new Phase 1 key can be renegotiated before the current one expires. The time for when this new key is negotiated before the current key expires can be set in the **Rekeymargin** field. In this example, leave the **Rekeymargin** as the default value of 10 minutes.

The **Rekeyfuzz** value refers to the maximum percentage by which the **Rekeymargin** should be randomly increased to randomize rekeying intervals. The **Key lifetimes** for both Phase 1 and Phase 2 are dependent on these values and must be greater that the value of "**Rekeymargin x (100 + Rekeyfuzz) / 100**." In this example, leave the **Rekeyfuzz** as the default value of 100%.

Enter a secret in the **Preshared Secret** field. Keep a record of this secret as it will be used to configure the remote party's secret. In this example, enter: **This secret must be kept confidential.**

***Warning***

*The secret must be entered identically at each end of the tunnel. The tunnel will fail to connect if the secret is not identical at both ends. The secret is a highly sensitive piece of information. It is essential to keep this information confidential. Communications over the IPSec tunnel may be compromised if this information is divulged.*

Select a **Phase 1 Proposal**. Any combination of the ciphers, hashes and Diffie Hellman groups that the SnapGear appliance supports can be selected. The supported ciphers are *DES* (56 bits), *3DES* (168 bits) and *AES* (128, 196 and 256 bits). The supported hashes are *MD5* and *SHA* and the supported Diffie Hellman groups are *1* (768 bit), *2* (1024 bit) and *5* (1536 bits). The SnapGear appliance also supports extensions to the Diffie Hellman groups to include 2048, 3072 and 4096 bit Oakley groups. In this example, select the **3DES-SHA-Diffie Hellman Group 2 (1024 bit)** option. Click the **Continue** button to configure the **Phase 2 Settings**.

## Other Options

The following options will become available on this page depending on what has been configured previously:

- **Local Public Key** field is the public part of the RSA key generated for RSA Digital Signatures authentication. These fields are automatically populated and do not need to be modified unless a different RSA key is to be used. This key must be entered in the Remote Public Key field of the remote party's tunnel configuration. This field appears when **RSA Digital Signatures** has been selected.

- **Remote Public Key** field is the public part of the remote party's RSA Key generated for RSA Digital Key authentication. This field must be populated with the remote party's public RSA key. This field appears when **RSA Digital Signatures** has been selected.

- **Modulus**, **Public Exponent**, **Private Exponent**, **Prime1**, **Prime2**, **Exponent1**, **Exponent2** and **Coefficient** fields constitute the private part of the RSA key. These fields are automatically populated and do not need to be modified unless a different RSA key is to be used. This field appears when **RSA Digital Signatures** has been selected.

- **Local Certificate** pull down menu contains a list of the local certificates that have been uploaded for x.509 authentication. Select the required certificate to be used to negotiate the tunnel. This field appears when **x.509 Certificates** has been selected.

Phase 2 Settings Page

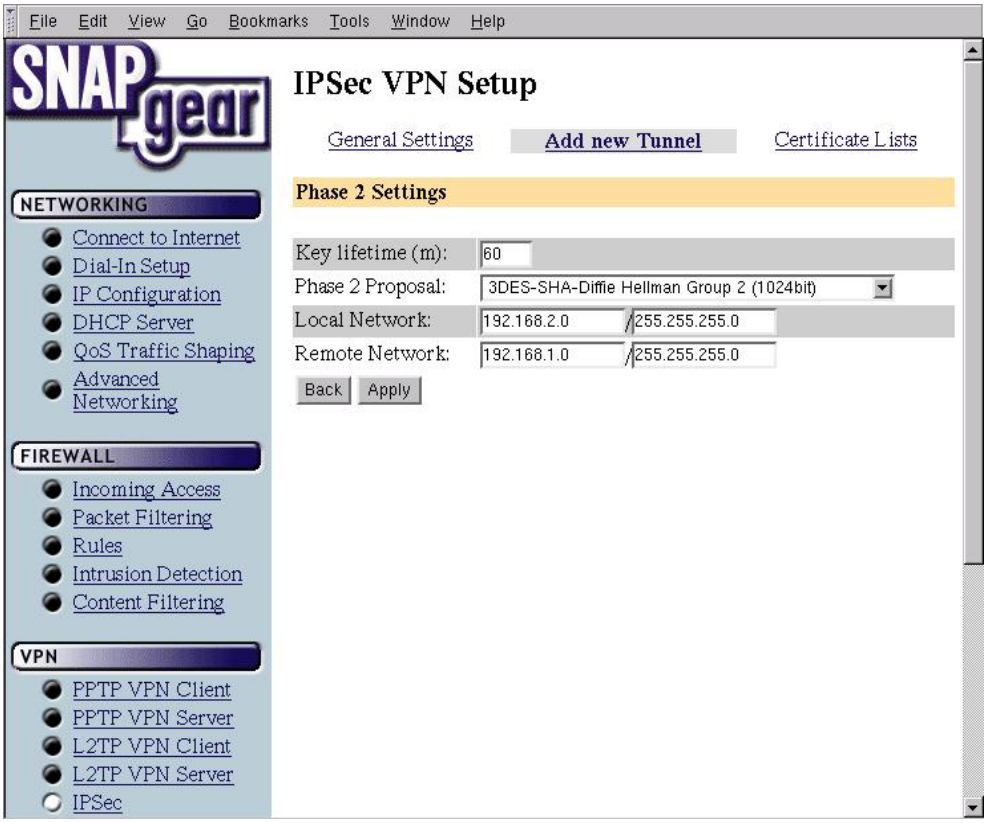



**Figure 8.18 Phase 2 Settings**

Set the length of time before Phase 2 is renegotiated in the **Key lifetime (m)** field. The length may vary between 1 and 1440 minutes. For most applications 60 minutes is recommended. In this example, leave the **Key Lifetime** as the default value of 60 minutes.

Select a **Phase 2 Proposal**. Any combination of the ciphers, hashes and Diffie Hellman groups that the SnapGear supports can be selected. The supported ciphers are *DES*, *3DES* and *AES* (128, 196 and 256 bits). The supported hashes are *MD5* and *SHA* and the supported Diffie Hellman group are *1* (768 bit), *2* (1024 bit) and *5* (1536 bits). The SnapGear also supports extensions to the Diffie Hellman groups to include 2048, 3072 and 4096 bit Oakley groups. *Perfect Forward Secrecy* is enabled if a Diffie-Hellman group or an extension is chosen. Phase 2 can also have the option to not select a Diffie Hellman Group, in this case *Perfect Forward Secrecy* is not enabled. *Perfect Forward Secrecy* of keys provides greater security and is the recommended setting. In this example, select the **3DES-SHA-Diffie Hellman Group 2** (1024 bit) option.

Define the **Local Network** behind the SnapGear appliance that is to have access through the tunnel. In this example, enter **192.168.2.0 / 255.255.255.0** in the field.

Define the **Remote Network** behind the remote party that is to have access through the tunnel. In this example, enter **192.168.1.0 / 255.255.255.0** in the field.

Click the **Apply** button to save the tunnel configuration.

## Other Options

The following options will become available on this page depending on what has been configured previously:

A separate section may appear to enter multiple **Local Networks** or **Remote Networks** or both. In the case where both local and remote parties have been configured to have multiple subnets behind them, a window similar to the following will be displayed.

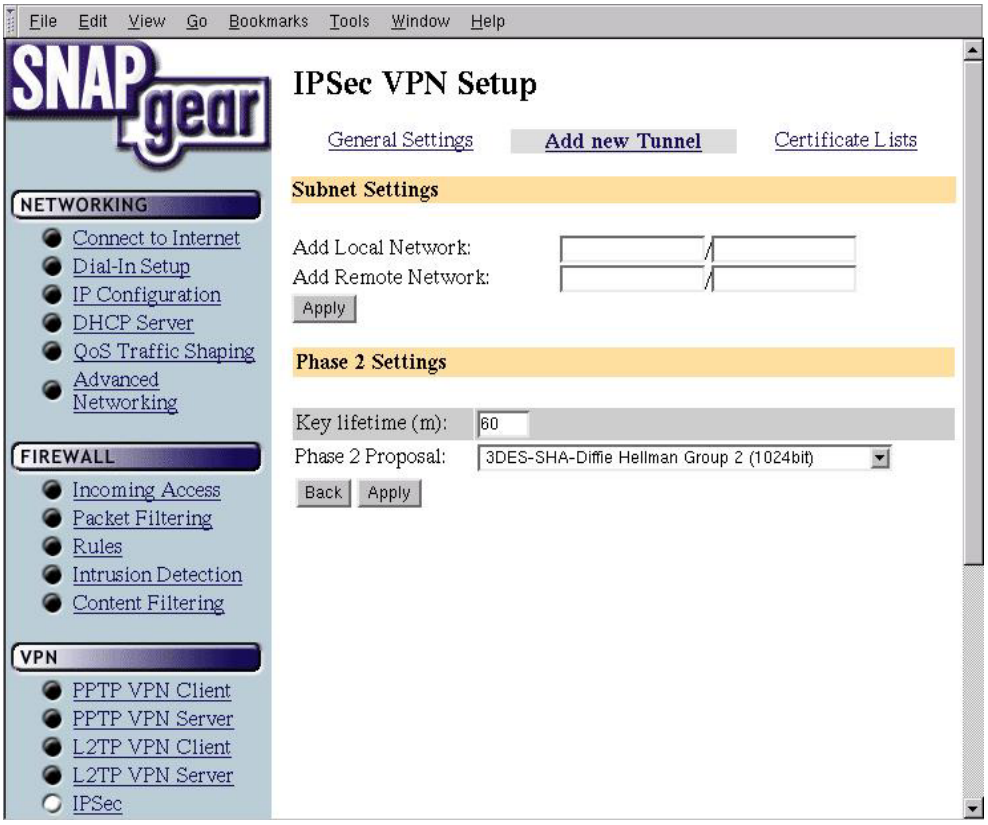



**Figure 8.19 Subnet Settings**

In the **Subnet Settings** section, a local and remote network combination can be added one at a time by entering subnets into the **Add Local Network** and **Add Remote Network** fields and then clicking **Apply**. Configured local and remote network combinations can be deleted by clicking the **Delete** checkbox for the appropriate combination and then clicking **Apply**. Once the required networks have been added, configure the **Phase 2 Settings** section.

# Configuring the headquarters SnapGear appliance

## Enabling IPSec

Click the **IPSec** link on the left side of the *SnapGear Management Console* web administration pages.

Check the **Enable IPSec** checkbox.

Select the type of IPSec endpoint the SnapGear has on its Internet interface. In this example, select **static IP address**.

Leave the **Set the IPSec MTU to be** checkbox unchecked.

Click the **Apply** button to save the changes.

## Configuring a tunnel to accept connections from the branch office

To create an IPSec tunnel, click the **IPSec** link on the left side of the *SnapGear Management Console* web administration pages, then click the **Add New Tunnel** tab at the top of the window. Many of the settings such as the **Preshared Secret**, **Phase 1** and **2 Proposals** and **Key Lifetimes** will be the same as the branch office.

## Tunnel Settings Page

Fill in the **Tunnel name** field with an apt description of the tunnel. The name must not contain spaces or start with a number. In this example, enter: *Branch_Office*

Leave checked the **Enable this tunnel** checkbox.

Select the Internet interface the IPSec tunnel is to go out on. In this example, select **default gateway interface** option.

Select the type of keying the tunnel will use. In this example, select the **Aggressive mode with Automatic Keying (IKE)** option.

Select the type of IPSec endpoint the remote party has. In this example, select the **dynamic IP address** option.

Select the type of authentication the tunnel will use. In this example, select the **Preshared Secret** option.

Select the type of private network that is behind the SnapGear appliance. In this example the Headquarters has a single network, so select the **single network behind this SnapGear** option.

Select whether the remote party is a single host or whether it is a gateway that has a single or has multiple networks behind it. In this example the Branch Office has single network, so select the **single network behind a gateway** option.

Select the type of routing the tunnel will be used as. In this example, select the **be a route to the remote party** option.

Click the **Continue** button to configure the **Local Endpoint Settings**.

### Local Endpoint Settings Page

Leave the **Optional Endpoint ID** field blank in this example. It is optional because the SnapGear appliance has a static IP address. If the remote party is a SnapGear appliance and an Endpoint ID is used, it must have the form *abcd@efgh*. If the remote party is not a SnapGear appliance refer the interoperability documents on the SnapGear knowledge base (**`http://www.snapgear.com/knowledgebase.html`**) to determine what form it must take.

Leave the **Enable IP Payload Compression** checkbox unchecked.

Leave the **Enable Phase 1 & 2 rekeying to be initiated from my end** checkbox checked.

Click the **Continue** button to configure the **Remote Endpoint Settings**.

### Remote Endpoint Settings Page

Enter the **Required Endpoint ID** of the remote party. In this example, enter the **Local Endpoint ID** at the Branch Office which was: **branch@office**

Click the **Continue** button to configure the **Phase 1 Settings**.

### Phase 1 Settings Page

Set the length of time before Phase 1 is renegotiated in the **Key lifetime (m)** field. In this example, leave the **Key Lifetime** as the default value of 60 minutes.

Set the time for when the new key is negotiated before the current key expires in the **Rekeymargin** field. In this example, leave the **Rekeymargin** as the default value of 10 minutes.

Set the maximum percentage by which the **Rekeymargin** should be randomly increased to randomize rekeying intervals in the **Rekeyfuzz** field. The **Key lifetimes** for both Phase 1 and Phase 2 are dependent on these values and must be greater that the value of "**Rekeymargin x (100 + Rekeyfuzz) / 100**." In this example, leave the **Rekeyfuzz** as the default value of 100%.

Enter a secret in the **Preshared Secret** field. This must remain confidential. In this example, enter the Preshared Secret used at the branch office SnapGear appliance, which was: **This secret must be kept confidential.**

Select a **Phase 1 Proposal**. In this example, select the **3DES-SHA-Diffie Hellman Group 2 (1024 bit)** option (same as the Branch Office **Phase 1 Proposal**).

Click the **Continue** button to configure the **Phase 2 Settings**.

### Phase 2 Settings Page

Set the length of time before Phase 2 is renegotiated in the **Key lifetime (m)** field. In this example, leave the **Key Lifetime** as the default value of 60 minutes.

Select a **Phase 2 Proposal**. In this example, select the **3DES-SHA-Diffie Hellman Group 2 (1024 bit)** option (same as the Branch Ofiice **Phase 2 Proposal**).

Define the **Local Network** behind the SnapGear that is to have access through the tunnel. In this example, enter **192.168.1.0 / 255.255.255.0** in the field.

Define the **Remote Network** behind the remote party that is to have access through the tunnel. In this example, enter **192.168.2.0 / 255.255.255.0** in the field.

Click the **Apply** button to save the tunnel configuration.

# Tunnel List

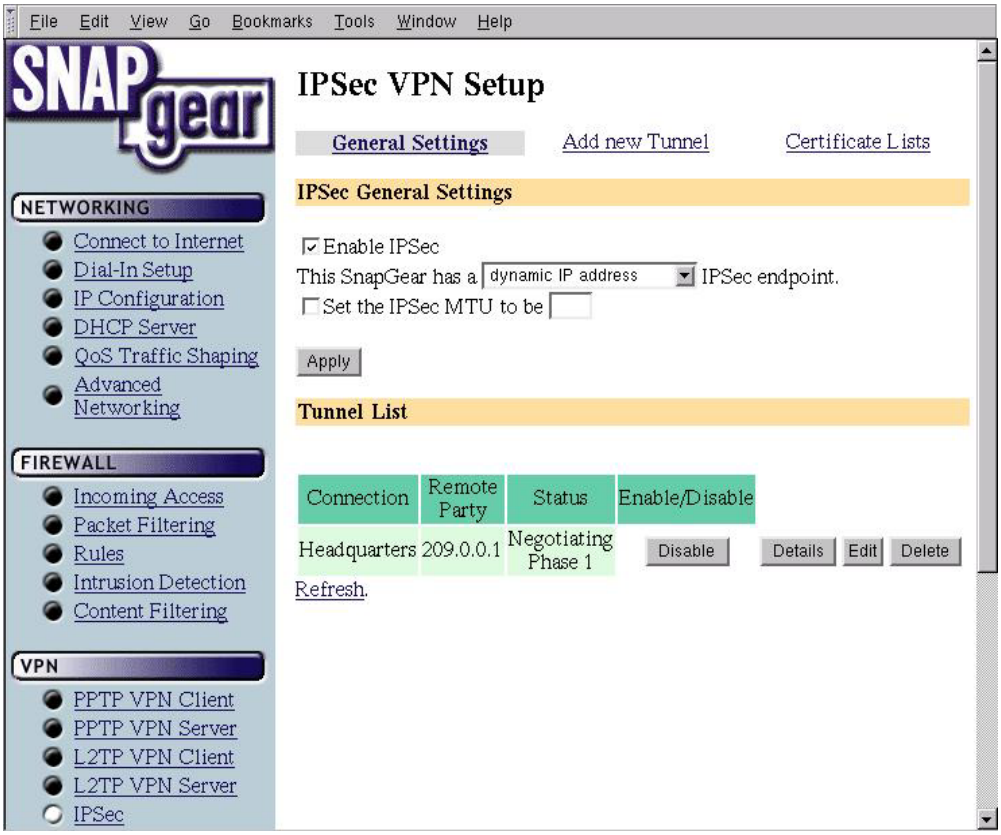



**Figure 8.20 Tunnel List**

## Connection

Once a tunnel has been configured, an entry with the tunnel name in the **Connection** field will be shown.

## Remote Party

The **Remote Party** which the tunnel is configured to connect to will be defined either by its Endpoint ID, IP Address or Distinguished Name.

## Status

Tunnels that use *Automatic Keying (IKE)* will have one of four states in the **Status** field. The states include the following:

- **Down** indicates that the tunnel is not being negotiated. This may be due to the following reasons:
    - IPSec is disabled.
    - The tunnel is disabled.
    - The tunnel could not be loaded due to misconfiguration.
- **Negotiating Phase 1** indicates that IPSec is negotiating Phase 1 to establish the tunnel. Aggressive or Main mode packets (depending on tunnel configuration) are transmitted during this stage of the negotiation process.
- **Negotiating Phase 2** indicates that IPSec is negotiating Phase 2 to establish the tunnel. Quick mode packets are transmitted during this stage of the negotiation process.
- **Running** indicates that the tunnel has been established.

Tunnels that use *Manual Keying* will either be in a **Down** or **Running** state.

### Enable/Disable

Each tunnel can be enabled or disabled by clicking on the **Enable** or **Disable** button under the **Enable/Disable** heading.

### Details

For tunnels that use *Automatic Keying*, further negotiation details can be seen by clicking the **Details** button. A window similar to the following will be displayed.

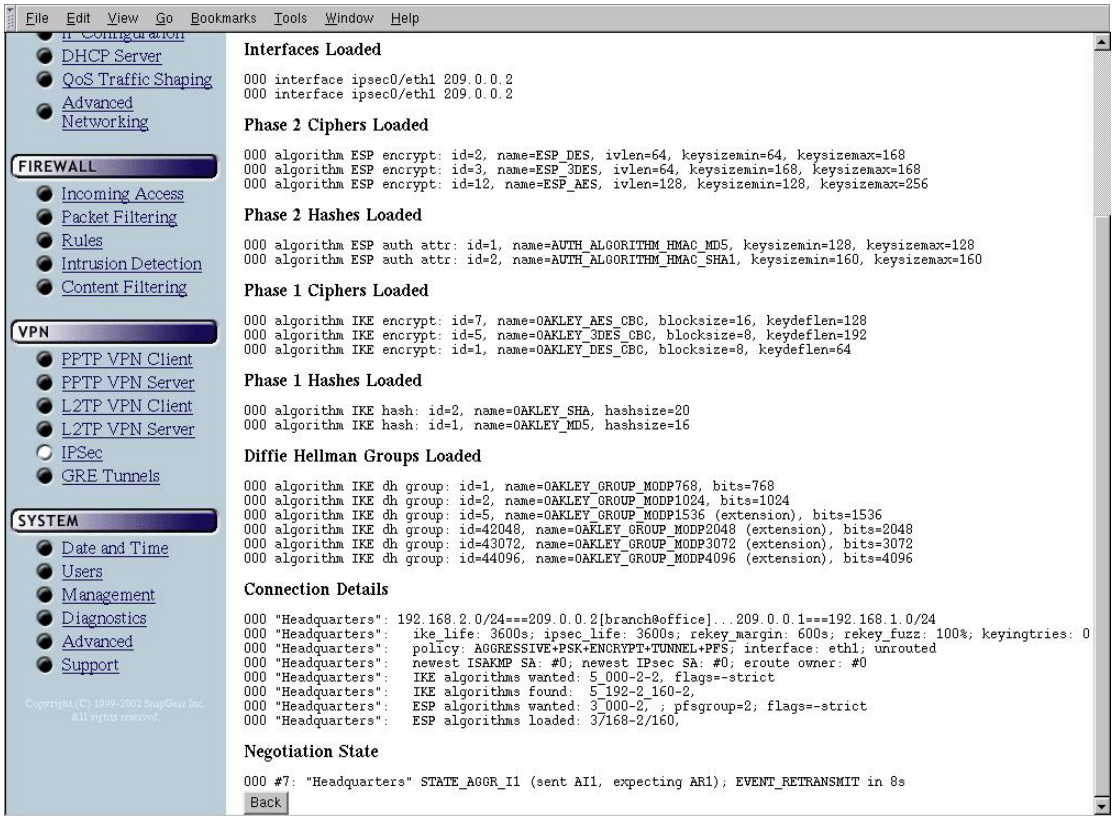

File Edit View Go Bookmarks Tools Window Help
DHCP Server
QoS Traffic Shaping
Advanced Networking
FIREWALL
Incoming Access
Packet Filtering
Rules
Intrusion Detection
Content Filtering
VPN
PPTP VPN Client
PPTP VPN Server
L2TP VPN Client
L2TP VPN Server
IPSec
GRE Tunnels
SYSTEM
Date and Time
Users
Management
Diagnostics
Advanced
Support
Interfaces Loaded
000 interface ipsec0/eth1 209.0.0.2
000 interface ipsec0/eth1 209.0.0.2
Phase 2 Ciphers Loaded
000 algorithm ESP encrypt: id=2, name=ESP_DES, ivlen=64, keysizemin=64, keysizemax=168
000 algorithm ESP encrypt: id=3, name=ESP_3DES, ivlen=64, keysizemin=168, keysizemax=168
000 algorithm ESP encrypt: id=12, name=ESP_AES, ivlen=128, keysizemin=128, keysizemax=256
Phase 2 Hashes Loaded
000 algorithm ESP auth attr: id=1, name=AUTH_ALGORITHM_HMAC_MD5, keysizemin=128, keysizemax=128
000 algorithm ESP auth attr: id=2, name=AUTH_ALGORITHM_HMAC_SHA1, keysizemin=160, keysizemax=160
Phase 1 Ciphers Loaded
000 algorithm IKE encrypt: id=7, name=OAKLEY_AES_CBC, blocksize=16, keydeflen=128
000 algorithm IKE encrypt: id=5, name=OAKLEY_3DES_CBC, blocksize=8, keydeflen=192
000 algorithm IKE encrypt: id=1, name=OAKLEY_DES_CBC, blocksize=8, keydeflen=64
Phase 1 Hashes Loaded
000 algorithm IKE hash: id=2, name=OAKLEY_SHA, hashsize=20
000 algorithm IKE hash: id=1, name=OAKLEY_MD5, hashsize=16
Diffie Hellman Groups Loaded
000 algorithm IKE dh group: id=1, name=OAKLEY_GROUP_MODP768, bits=768
000 algorithm IKE dh group: id=2, name=OAKLEY_GROUP_MODP1024, bits=1024
000 algorithm IKE dh group: id=5, name=OAKLEY_GROUP_MODP1536 (extension), bits=1536
000 algorithm IKE dh group: id=42048, name=OAKLEY_GROUP_MODP2048 (extension), bits=2048
000 algorithm IKE dh group: id=43072, name=OAKLEY_GROUP_MODP3072 (extension), bits=3072
000 algorithm IKE dh group: id=44096, name=OAKLEY_GROUP_MODP4096 (extension), bits=4096
Connection Details
000 "Headquarters": 192.168.2.0/24===209.0.0.2[branch@office]...209.0.0.1===192.168.1.0/24
000 "Headquarters": ike_life: 3600s; ipsec_life: 3600s; rekey_margin: 600s; rekey_fuzz: 100%; keyingtries: 0
000 "Headquarters": policy: AGGRESSIVE+PSK+ENCRYPT+TUNNEL+PFS; interface: eth1; unrouted
000 "Headquarters": newest ISAKMP SA: #0; newest IPsec SA: #0; eroute owner: #0
000 "Headquarters": IKE algorithms wanted: 5_000-2-2, flags=-strict
000 "Headquarters": IKE algorithms found: 5_192-2_160-2,
000 "Headquarters": ESP algorithms wanted: 3_000-2, ; pfsgroup=2; flags=-strict
000 "Headquarters": ESP algorithms loaded: 3/168-2/160,
Negotiation State
000 #7: "Headquarters" STATE_AGGR_I1 (sent AI1, expecting AR1); EVENT_RETRANSMIT in 8s
Back

**Figure 8.21 Negotiation Details**

**Interfaces Loaded** lists the SnapGear appliance's interfaces which IPSec will use.

**Phase 2 Ciphers Loaded** lists the encryption ciphers that tunnels can be configured with for Phase 2 negotiations. This will include DES, 3DES and AES.

**Phase 2 Hashes Loaded** lists the authentication hashes that tunnels can be configured with for Phase 2 negotiations. This will include MD5 and SHA1 (otherwise known as SHA).

**Phase 1 Ciphers Loaded** lists the encryption ciphers that tunnels can be configured with for Phase 1 negotiations. This will include DES, 3DES and AES.

**Phase 1 Hashes Loaded** lists the authentication hashes that tunnels can be configured with for Phase 1 negotiations. This will include MD5 and SHA.

**Diffie Hellman Groups Loaded** lists the Diffie Hellman groups and Oakley group extensions that can be configured for both Phase 1 and Phase 2 negotiations.

**Connection Details** lists an overview of the tunnel's configuration. It contains the following information:

- An outline of the tunnel's network setup. In this example, it is *192.168.2.0/24===209.0.0.2(branch@office)...209.0.0.1===192.168.1.0/24*

- Phase 1 and Phase 2 key lifetimes (**ike_life** and **ipsec_life** respectively). In this example, they are both *3600s*.

- Type of automatic (IKE) keying. In this example, the **policy** line has: *AGGRESSIVE*. For Main mode, it will read *MAIN*.

- Type of authentication used. In this example, the **policy** line has: *PSK* (Preshared Key). For RSA Digital Signatures or x.509 certificates, it will read *RSA*.

- Whether Perfect Forward Secrecy is used. In this example, the **policy** line has the *PFS* keyword. If PFS is disabled, then the keyword will not appear.

- Whether IP Payload Compression is used. In this example, the **policy** line does not have the *COMPRESS* keyword since it has not been enabled.

- The interface on which the tunnel is going out. In this example, the **interface** line has *eth1*, which is the Internet interface.

- The current Phase 1 key. This is the number that corresponds to the **newest ISAKMP SA** field. In this example, phase 1 has not be successfully negotiated, so there is no key yet.

- The current Phase 2 key. This is the number that corresponds to the **newest IPSec SA** field. In this example, phase 1 has not be successfully negotiated, so there is no key yet.

- The Phase 1 proposal wanted. The line **IKE algorithms wanted** reads *5_000-2-2*. The *5_000* refers to cipher 3DES (where 3DES has an id of 5, see Phase 1 Ciphers Loaded), the first *2* refer to hash SHA (where SHA has an id of 2, see Phase 1 Hashes Loaded) and the second *2* refer to the Diffie Hellman Group 2 (where Diffie Hellman Group 2 has an id of 2).

- The Phase 2 proposal wanted. The line **ESP algorithms wanted** reads *3_000-2; pfsgroup=2*. The *3_000* refers to cipher 3DES (where 3DES has an id of 3, see Phase 2 Ciphers Loaded), the *2* refers to hash SHA1 or SHA (where SHA1 has an id of 2, see Phase 2 Hashes Loaded) and *pfsgroup=2* refers to the Diffie Hellman Group 2 for Perfect Forward Secrecy (where Diffie Hellman Group 2 has an id of 2).

**Negotiation State** reports what stage of the negotiation process the tunnel is in. In this example it has *initiated* and sent the first aggressive mode packet (*AI1*) and is expecting its *response* (*AR1*) in the line *STATE_AGGR_I1 (sent AI1, expecting AR1)*. Once the Phase 1 has been successfully negotiated, the status will have the line *ISAKMP SA established*. Once the Phase 2 has been successfully negotiated, the status will read *IPSec SA established*. The tunnel will then be established and running.

Edit

The configuration for each tunnel can be modified by clicking the **Edit** button.

Delete

The configuration for each tunnel can be removed from the SnapGear appliance by clicking the **Delete** button.

## NAT Traversal Support

NAT Traversal allows tunnels to be established when the IPSec endpoints reside behind NAT devices. If any NAT devices are detected, the NAT Traversal feature is automatically used. It cannot be configured manually on the SnapGear appliance.

## Dynamic DNS Support

Internet Service Providers generally charge higher fees for static IP addresses than for dynamic IP addresses when connecting to the Internet. The SnapGear appliance can reduce costs since it allows tunnels to be established with both IPSec endpoints having dynamic IP addresses. The two endpoints must, however, be SnapGear appliances and at least one end must have *dynamic DNS* enabled. The SnapGear appliance supports a number of dynamic DNS providers. When configuring the tunnel, select the **DNS hostname address** type for the IPSec endpoint that has dynamic DNS supported and enable **Dead Peer Detection**. If the IP address of the SnapGear appliance's DNS hostname changes, the tunnel will automatically renegotiate and establish the tunnel.

# Certificate Management

*x.509 Certificates* can be used to authenticate IPSec endpoints during tunnel negotiation for Automatic Keying. The other methods are *Preshared Secrets* and *RSA Digital Signatures*.

Certificates need to be uploaded to the SnapGear appliance before they can be used in a tunnel. Certificates have time durations in which they are valid. Ensure that the certificates uploaded are valid and that the **Date and Time** settings have been set correctly on the SnapGear appliance.

The SnapGear appliance only supports certificates in *base64 PEM* or *binary DER* format. Some Certificate Authorities (CA) distribute certificates in a *PKCS#12* format file and the CA, local public key and private key certificates must be extracted or created before uploading them into the SnapGear appliance.

## Extracting certificates

Use the *openssl* application tool on the SnapGear CD to extract these certificates (ensure the *cygwin1.dll* library is in the same directory as the *openssl* application). To extract the CA certificate, enter the following at the Windows command prompt:

**openssl pkcs12 -nomacver -cacerts -nokeys -in pkcs12_file -out ca_certificate.pem**

.. where **pksc12_file** is the PKCS#12 file issued by the CA and **ca_certificate.pem** is the CA certificate to be uploaded into the SnapGear appliance.

The application will prompt you to **Enter Import Password**. Enter the password used to create the certificate. If none was used simply press enter.

To extract the local public key certificate type, enter the following at the Windows command prompt:

**openssl pkcs12 -nomacver -clcerts -nokeys -in pkcs12_file -out local_certificate.pem**

.. where **pksc12_file** is the PKCS#12 file issued by the CA and **local_certificate.pem** is the local public key certificate to be uploaded into the SnapGear appliance.

The application will prompt you to **Enter Import Password**. Enter the password used to create the certificate. If none was used simply press enter.

To extract the local private key certificate type, enter the following at the Windows command prompt:

**openssl pkcs12 -nomacver -nocerts -in pkcs12_file -out local_private_key.pem**

.. where **pksc12_file** is the PKCS#12 file issued by the CA and **local_private_key.pem** is the local private key certificate to be uploaded into the SnapGear appliance.

The application will prompt you to **Enter Import Password**. Enter the password used to create the certificate. If none was used simply press enter. The application will also prompt you to **Enter PEM pass phrase** which is the pass phrase used to secure the private key file. Choose a secure pass phrase that is greater than 4 characters long and this will be the same pass phrase entered when uploading the private key certificate into the SnapGear appliance. The application will then prompt you to verify the pass phrase again. Simply type it in again.

The SnapGear appliance also supports *Control Revocation List* (CRL) files. A CRL is a list of certificates that have been revoked by the CA before they expired. This may be necessary if the private key certificate has been compromised or if the holder of the certificate is to be denied the ability to establish a tunnel to the SnapGear appliance.

## Creating Certificates

The first thing necessary is to create a Certificate Authority (CA).

1. Create the CA directory:

   **mkdir rootCA**

2. Create the serial number for the first certificate:

   **echo 01 > rootCA/serial**

3. Create an empty CA database file:

   linux: **touch rootCA/index.txt**

   Windows: **type nul > rootCA/index.txt**

4. Create the self-signed root CA certificate:

   **openssl req -config openssl.cnf -new -x509 -keyout rootCA/ca.key -out rootCA/ca.pem -days** *DAYS_VALID* **-nodes**

   .. where *DAYS_VALID* is the number of days the root CA is valid for.

   Remove the **–nodes** option if you want to use a password to secure the CA key.

For each certificate you wish to create, there are two steps:

1. Create the certificate request:

   **openssl req -config openssl.cnf -new -keyout cert1.key -out cert1.req**

   Enter a PEM pass phrase (this is the same pass phrase required when you upload the key to the SnapGear appliance) and then the certificate details. All but the **Common Name** are optional and may be omitted.

2. Sign the certificate request with the CA :

   **openssl ca -config openssl.cnf -out cert1.pem -notext -infiles cert1.req**

Then you will have a certificate/key pair, *cert1.pem* and *cert1.key*, ready to use in the SnapGear appliance.

For each certificate required, change the *cert1.** filenames appropriately.

## Adding Certificates

To add certificates to the SnapGear appliance, click the **IPSec** link on the left side of the *SnapGear Management Console* web administration pages and then click the **Certificate Lists** tab at the top of the window. A window similar to the following will be displayed.

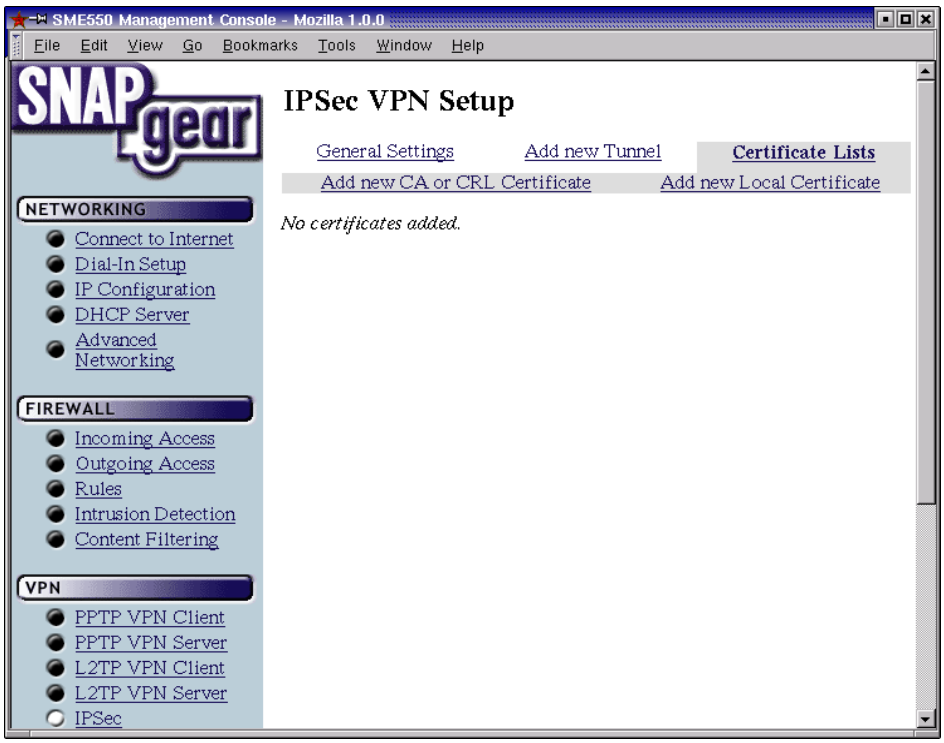



**Figure 8.22 Adding certificates**

## Adding a CA or CRL Certificate

Click the **Add new CA or CRL Certificate** tab. A window similar to the following will be displayed.

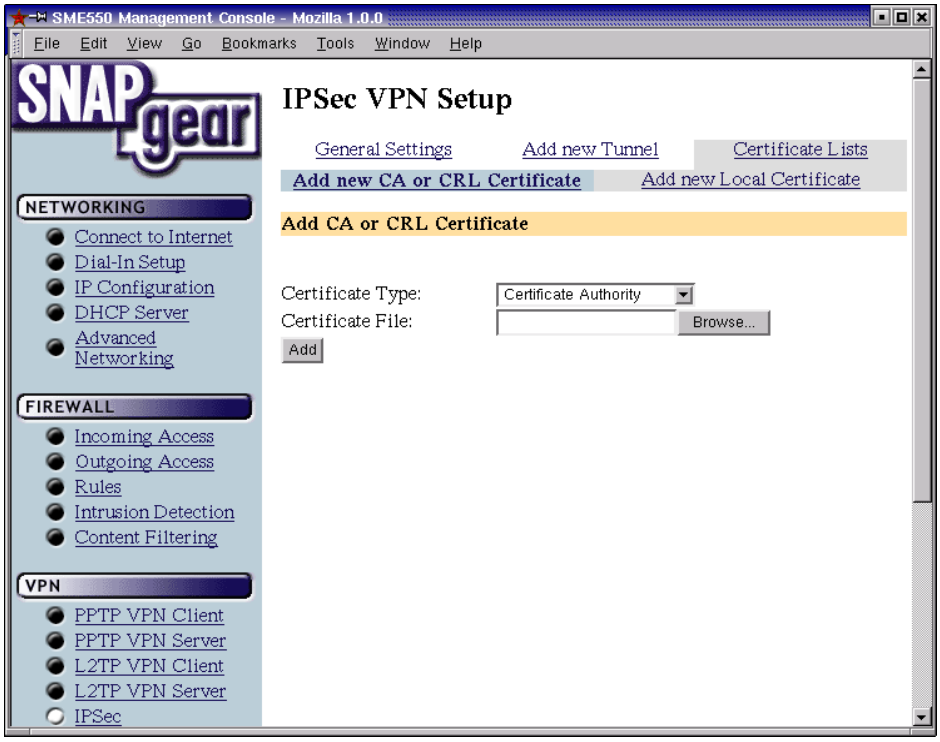



**Figure 8.23 Add new CA or CRL Certificate**

Select whether a **Certificate Authority** or **Control Revocation List** certificate is to be uploaded from the **Certificate Type** pull down menu.

Enter the *Certificate Authority's Public Key certificate* or *CRL* file in the **Certificate File** field. Click the **Browse** button to select the file from the host computer. CA Certificates have time durations in which they are valid. Ensure that the certificates uploaded are valid and that the **Date and Time** has been set correctly on the SnapGear appliance. Also ensure that the certificate is in *PEM* or *DER* format.

Click the **Add** button to upload the file.

## Adding a Local Certificate

1 Click the **Add new Local Certificate** tab. A window similar to the following will be displayed.

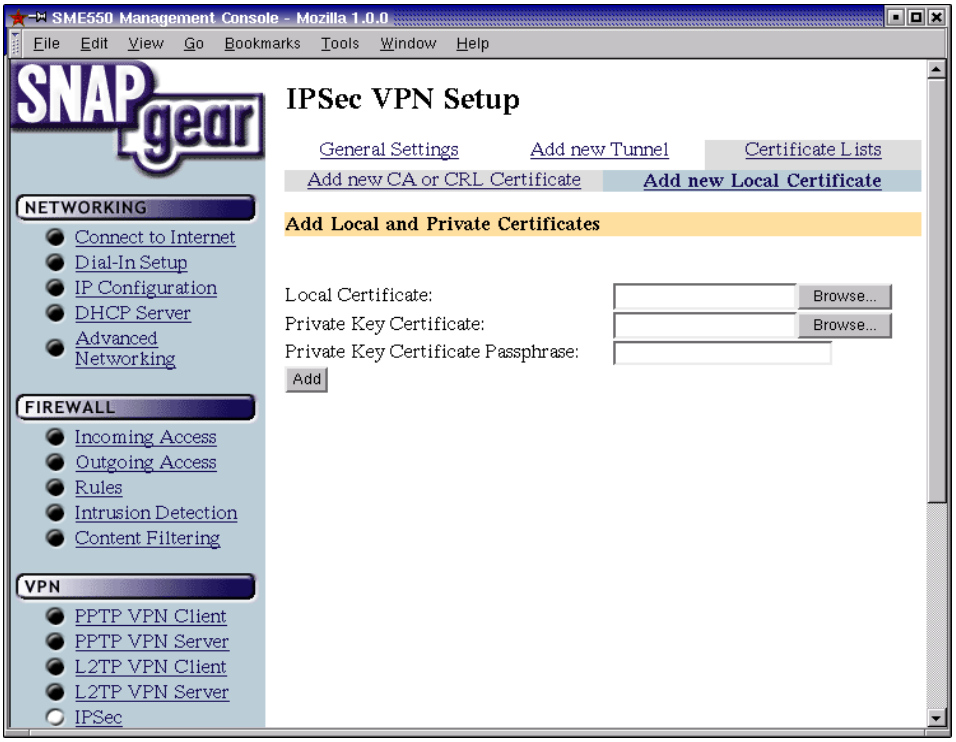



**Figure 8.24 Add new Local Certificate**

Enter the *Local Public Key certificate* in the **Local Certificate** field. Click the **Browse** button to select the file from the host computer. Certificates have time durations in which they are valid. Ensure that the certificates uploaded are valid and that the **Date and Time** settings have been set correctly on the SnapGear appliance. Also ensure that the certificate is in *PEM* or *DER* format.

Enter the *Local Private Key certificate* in the **Private Key Certificate** field. Click the **Browse** button to select the file from the host computer. Ensure the certificate is the private key for the above public key certificate. Also ensure that the certificate is in *PEM* or *DER* format.

Enter the passphrase to unlock the private key certificate in the **Private Key Certificate Passphrase** field.

Click the **Add** button to upload the certificates and passphrase.

Once a CA and local certificate has been uploaded, a window similar to the following will be displayed.

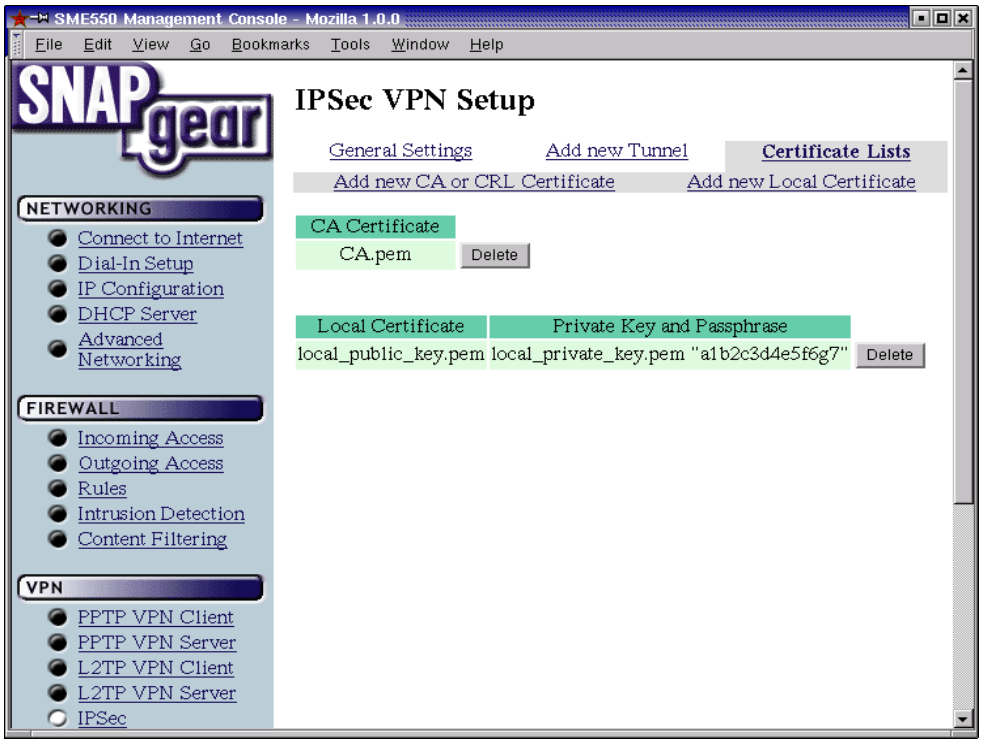



**Figure 8.25 CA and local certificate**

The certificate names will be displayed under the appropriate certificate type. Clicking the **Delete** button deletes the certificate from the SnapGear appliance.

# Troubleshooting

- **Symptom:** IPSec is not running and is enabled.

  **Possible Cause:** The SnapGear appliance has not been assigned a default gateway.

  **Solution:** Ensure the SnapGear appliance has a default gateway by configuring the Internet connection on the Connect to Internet page or assigning a default gateway on the IP Configuration page.

- **Symptom:** Tunnel is always down even though IPSec is running and the tunnel is enabled.

  **Possible Cause:** The tunnel is using Manual Keying and the encryption and/or authentication keys are incorrect.

The tunnel is using Manual Keying and the SnapGear appliance's and/or remote party's keys do not correspond to the Cipher and Hash specified.

**Solution:** Configure a correct set of encryption and/or authentication keys. Select the appropriate Cipher and Hash that the key have been generated from, or change the keys used to use the selected Cipher and Hash.

- **Symptom:** Tunnel is always Negotiating Phase 1.

  **Possible Cause:** The remote party does not have an Internet IP address (a *No route to host* message is reported in the system log).

  The remote party has IPSec disabled (a *Connection refused* message is reported in the system log).

  The remote party does not have a tunnel configured correctly because:

  - The tunnel has not been configured.
  - The Phase 1 proposals do not match.
  - The secrets do not match.
  - The RSA key signatures have been incorrectly configured.
  - The Distinguished Name of the remote party has not be configured correctly.
  - The Endpoint IDs do not match.
  - The remote IP address or DNS hostname has been incorrectly entered.
  - The certificates do not authenticate correctly against the CA certificate.

  **Solution:** Ensure that the tunnel settings for the SnapGear appliance and the remote party are configured correctly. Also ensure that both have IPSec enabled and have Internet IP addresses. Check that the CA has signed the certificates.

- **Symptom:** Tunnel is always Negotiating Phase 2

  **Possible Cause:** The Phase 2 proposals set for the SnapGear appliance and the remote party do not match.

  The local and remote subnets do not match.

  **Solution:** Ensure that the tunnel settings for the SnapGear appliance and the remote party are configured correctly.

- **Symptom:** Large packets don't seem to get transmitted

  **Possible Cause:** The MTU of the IPSec interface is too large.

  **Solution:** Reduce the MTU of the IPSec interface.

- **Symptom:** Tunnel goes down after a while

  **Possible Cause:** The remote party has gone down.

  The remote party has disabled IPSec.

  The remote party has disabled the tunnel.

  The tunnel on the SnapGear appliance has been configured not to rekey the tunnel.

  The remote party is not rekeying correctly with the SnapGear

  **Solution:** Confirm that the remote party has IPSec and the tunnel enabled and has an Internet IP address. Ensure that the SnapGear appliance has rekeying enabled. If the tunnel still goes down after a period of time, it may be due to the SnapGear appliance and remote party not recognising the need to renegotiate the tunnel. This situation arises when the remote party is configured to accept incoming tunnel connections (as opposed to initiate tunnel connections) and reboots. The tunnel has no ability to let the other party know that a tunnel renegotiation is required. This is an inherent drawback to the IPSec protocol. Different vendors have implemented their own proprietry method to support the ability to detect whether to renegotiate the tunnel. SnapGear has used the draft produced by Cisco Systems (*draft-ietf-ipsec-dpd-00.txt*) to implement dead peer detection. Unfortunately, unless the remote party implements this draft, the only method to renegotiate the tunnel is to reduce the key lifetimes for Phase 1 and Phase 2 for Automatic Keying (IKE). This does not occur for Manual Keying.

- **Symptom:** Dead Peer Detection does not seem to be working

  **Possible Cause:** The tunnel has Dead Peer Detection disabled.

  The remote party does not support Dead Peer Detection according to *draft-ietf-ipsec-dpd-00.txt*

  **Solution:** Enable Dead Peer Detection support for the tunnel. Unless the remote party supports *draft-ietf-ipsec-dpd-00.txt*, Dead Peer Detection will not be used.

- **Symptom:** Tunnels using x.509 certificate authentication do not work

  **Possible Cause:** The date and time settings on the SnapGear appliance has not been configured correctly.

  The certificates have expired.

  The Distinguished Name of the remote party has not be configured correctly on the SnapGear appliance's tunnel.

  The certificates do not authenticate correctly against the CA certificate.

  The remote party's settings are incorrect.

  **Solution:** Confirm that the certificates are valid. Confirm also that the remote party's tunnel settings are correct. Check the Distinguished Name entry in the the SnapGear appliance's tunnel configuration is correct.

- **Symptom:** Remote hosts can be accessed using IP address but not by name

  **Possible cause:** Windows network browsing broadcasts are not being transmitted through the tunnel.

  **Solution:** Set up a WINS server and use it to have the remote hosts resolve names to IP addresses.

  Set up LMHOST files on remote hosts to resolve names to IP adresses.

- **Symptom:** Tunnel comes up but the application does not work across the tunnel.

  **Possible cause:** There may be a firewall device blocking IPSec packets.

  The MTU of the IPSec interface may be too large.

  The application uses broadcasts packets to work.

  **Solution:** Confirm that the problem is the VPN tunnel and not the application being run. These are the steps you can try to find where the problem is (it is assumed that a network to network VPN is being used):

  Ping from your PC to the Internet IP address of the remote party (it assumed that the remote party is configured to accept incoming pings)

  Ping from your PC to the LAN IP address of the remote party.

  Ping from your PC to a PC on the LAN behind the remote party that the tunnel has been configured to combine.

  If you cannot ping the Internet IP address of the remote party, either the remote party is not online or your computer does not have its default gateway as the SnapGear appliance. If you can ping the Internet IP address of the remote party but not the LAN IP address, then the remote party's LAN IP address or its default gateway has not been configured properly. Also check your network configuration for any devices filtering IPSec packets (protocol 50) and whether your Internet Service Provider is filtering IPSec packets. If you can ping the LAN IP address of the remote party but not a host on the remote network, then either the local and/or remote subnets of the tunnel settings have been misconfigured or the remote host does not have its default gateway as the remote party.

  If you can ping across the tunnel, then check if the MTU of the IPSec interface is allowing packets to go through. Reduce the MTU if large packets are not being sent through the tunnel.

  If the application is still not working across the tunnel, then the problem is with the application. Check that the application uses IP and does not use broadcast packets since these will not be sent through the SnapGear appliance. You should contact the producer of the application for support.

# GRE

The GRE configuration of the SnapGear appliance allows you to build GRE tunnels to other devices that support the *Generic Routing Encapsulating* protocol. You can build GRE tunnels to other SnapGear appliances that support GRE, or to other devices such as Cisco equipment.

***Warning***

*GRE tunnels are not secure unless they are run over another secure protocol. Using a GRE tunnel that runs over the public Internet, it is possible for an attacker to put packets onto your network. If you want a secure tunneling mechanism, then you should use IPSec, or tunnel GRE over either IPSec or PPTP tunnels.*

## Setting up a GRE tunnel

To create a GRE tunnel to a remote device:

Specify the IP address that the remote GRE server is listening on in **Remote IP**. You can specify a domain name here.

Specify the IP address that you want the local GRE server to listen on in **Local IP**. You can enter any IP address here, but be aware that the GRE server will only respond to IP addresses, which correspond to the specified IP address.

Specify the IP address that you want to be associated with the local end of the GRE tunnel in **IP Address**.

Click **Add** when you are satisfied with the information you have supplied.

After you have created a new GRE endpoint, you can add routes to it. When the tunnel is started (done automatically on reboot or when a new tunnel is started), these routes are added to the GRE tunnel, so that packets destined for these networks are sent over the GRE tunnel.

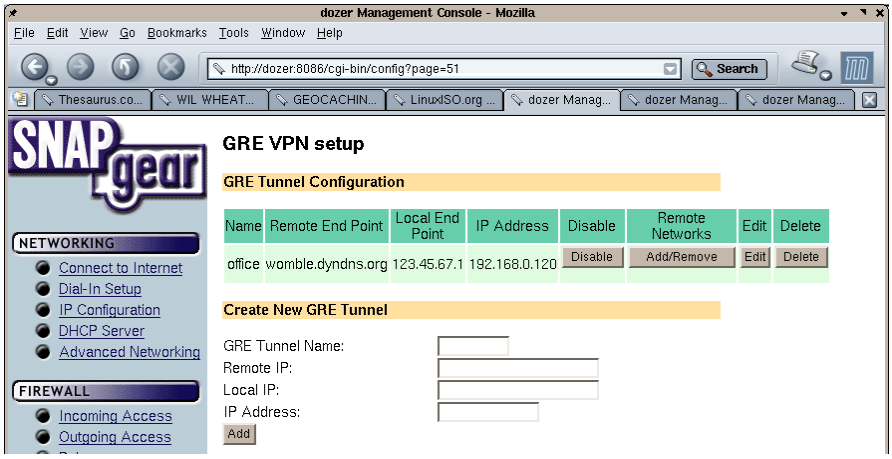



**Figure 8.26 GRE VPN setup**

## Troubleshooting

- **Symptom:** Cannot ping a host on the other side of the GRE tunnel.

  Ensure that there is a route set up on the GRE tunnel to the remote network.

  Ensure that there is a route on the remote GRE endpoint to the network at this end of the GRE tunnel.

  Check that there is a GRE interface created on the device. To do this, go into *Advanced Networking* and scroll to the bottom. There should be an interface called **gre***X* created. **gre***X* is the same as the **Interface Name** specified in the table of current GRE tunnels.

  Also ensure that the required routes have been set up on the GRE interface. This might not occur if you have the same route specified on different GRE tunnels, or on different network interfaces.

  Ensure that the remote GRE endpoint is reacheable. Do this by using the ping utility on the *Advanced Networking* page.

- **Symptom:** Cannot ping the remote GRE end point.

  Ensure that the remote GRE end point responds to pings. Note that by default no packets will be routed across the GRE tunnel unless there is a route setup on the GRE tunnel.

# L2TP

The *Layer Two Tunneling Protocol* was developed by Microsoft and Cisco as a multi-purpose network transport protocol.

Many DSL ISPs use L2TP over ATM to create tunnels across the Internet backbone. The SnapGear L2TP implementation can only run L2TP over Ethernet since it doesn't have an ATM adapter. L2TP packets are encapsulated in UDP packets on port 1701 and sent over Ethernet to the L2TP server.

## L2TP VPN Client

The SnapGear L2TP VPN client is configured and operates in a similar way to the PPTP VPN Client.

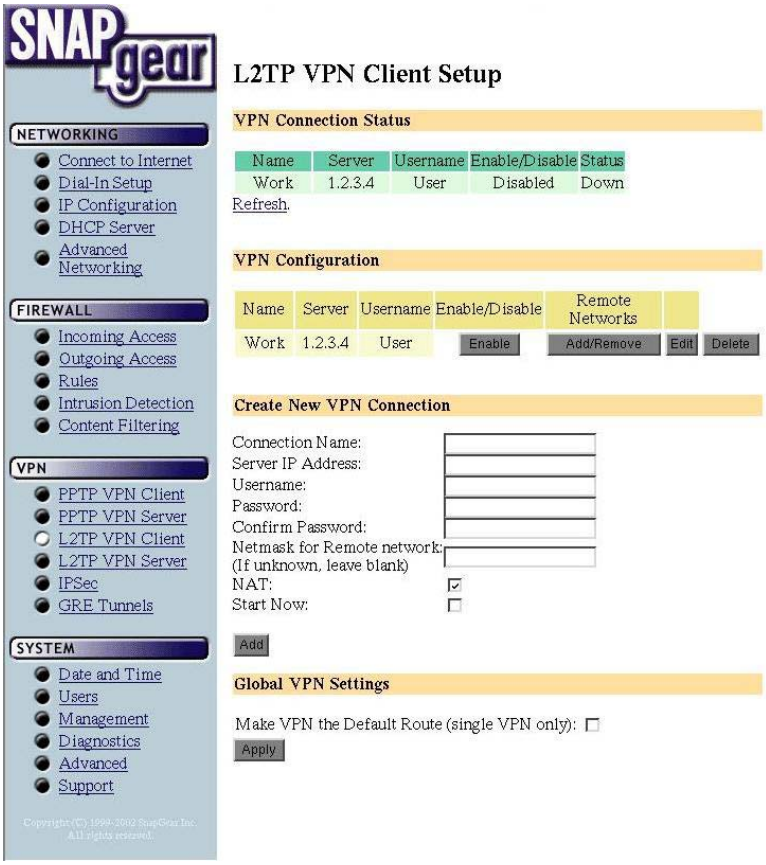



**Figure 8.27 L2TP VPN client setup**

## L2TP Server

The L2TP Server runs in a similar way to the PPTP Server. A range of IP addresses is allocated, and then username and password pairs are created to allow users to log-on.

***Note***

*To increase security, L2TP VPN connections from Windows PCs are also run through an IPSec tunnel. This means an IPSec connection must be configured and enabled on the SnapGear appliance as well as the L2TP server before Windows clients can connect.*

The default way for the IPSec connection to be authenticated is to use x.509/RSA certificates. The SnapGear appliance therefore needs to have IPSec configured with both a CA and local certificate before connections can be established. The Windows machine needs to have a copy of the CA certificate used to sign the SnapGear appliance's local certificate, and similarly, the SnapGear appliance needs a copy of the CA of the Windows certificate.

# 9. System

## Date and Time

### Set date and time

If you have a Javascript enabled web browser, you will be able to click the top **Set Date and Time** button to synchronize the time on the SnapGear appliance with that of your PC.

Alternately, you can manually set the **Year**, **Month**, **Date**, **Hour** and **Minute** using the selection boxes to set the date and time on the SnapGear appliance.

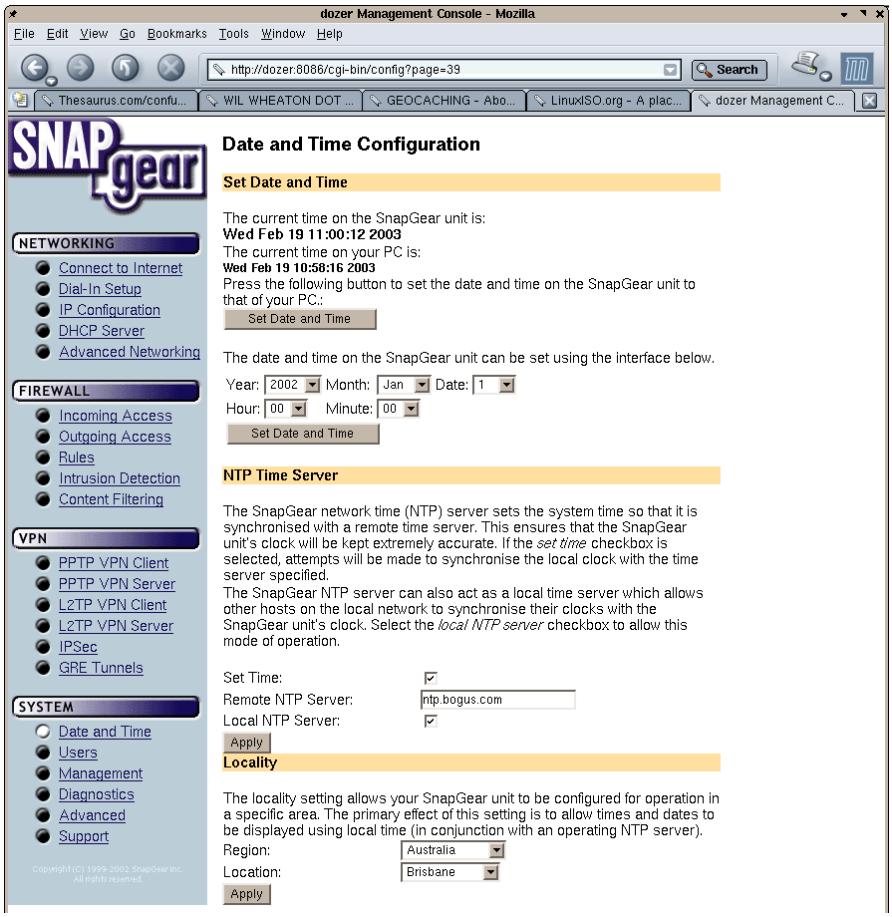

dozer Management Console - Mozilla
File Edit View Go Bookmarks Tools Window Help
http://dozer:8086/cgi-bin/config?page=39
Search
Thesaurus.com/confu...
WIL WHEATON DOT ...
GEOCACHING - Abo...
LinuxISO.org - A plac...
dozer Management C...
SNAPgear
NETWORKING
Connect to Internet
Dial-In Setup
IP Configuration
DHCP Server
Advanced Networking
FIREWALL
Incoming Access
Outgoing Access
Rules
Intrusion Detection
Content Filtering
VPN
PPTP VPN Client
PPTP VPN Server
L2TP VPN Client
L2TP VPN Server
IPSec
GRE Tunnels
SYSTEM
Date and Time
Users
Management
Diagnostics
Advanced
Support
Date and Time Configuration
Set Date and Time
The current time on the SnapGear unit is:
Wed Feb 19 11:00:12 2003
The current time on your PC is:
Wed Feb 19 10:58:16 2003
Press the following button to set the date and time on the SnapGear unit to that of your PC.:
Set Date and Time
The date and time on the SnapGear unit can be set using the interface below.
Year: 2002 Month: Jan Date: 1
Hour: 00 Minute: 00
Set Date and Time
NTP Time Server
The SnapGear network time (NTP) server sets the system time so that it is synchronised with a remote time server. This ensures that the SnapGear unit's clock will be kept extremely accurate. If the set time checkbox is selected, attempts will be made to synchronise the local clock with the time server specified.
The SnapGear NTP server can also act as a local time server which allows other hosts on the local network to synchronise their clocks with the SnapGear unit's clock. Select the local NTP server checkbox to allow this mode of operation.
Set Time:
Remote NTP Server: ntp.bogus.com
Local NTP Server:
Apply
Locality
The locality setting allows your SnapGear unit to be configured for operation in a specific area. The primary effect of this setting is to allow times and dates to be displayed using local time (in conjunction with an operating NTP server).
Region: Australia
Location: Brisbane
Apply

**Figure 9.1 Date and time configuration**

### NTP time server

The SnapGear appliance can synchronize its system time with a remote time server using the Network Time Protocol (NTP). Configuring the NTP time server ensures that the SnapGear appliance's clock (in UTC) will be accurate soon after the Internet connection is established. If NTP is not used, the system clock will be set randomly when the SnapGear appliance starts up.

To set the system time using NTP, select the **Set Time** checkbox on the **NTP Server Configuration** page and enter the IP address of the time server in the **Remote NTP Server** field.

### Locality

Select your region then select your location within said region. The system clock will subsequently show local time. Without setting this, the system clock will show UTP. Setting a time zone is only relevant if you are synchronizing with an NTP server or your SnapGear appliance has a real time clock. Without either of these, the SnapGear appliance's clock is set randomly at startup.

## Users

User accounts on a SnapGear appliance allow administrative duties to be spread amongst a number of different people according to their level of competence and trust. Each user on the SnapGear appliance has a password that they use to authenticate themselves to the unit's web pages. They also have a number of access controls that modify what they can and cannot do via the web interface.

There is one special user, *root*, who has the role of the final administrative user. This user has extra capabilities beyond any other user.

User access controls are grouped into four broad categories. The *root* administrative user by default has permission to perform any action on the SnapGear appliance. Other users default to no permission. All users can have their access controls modified (including *root*). To fully utilize access controls, the *root* user should have their access controls turned off and other users create to handle the day to day administrative duties.

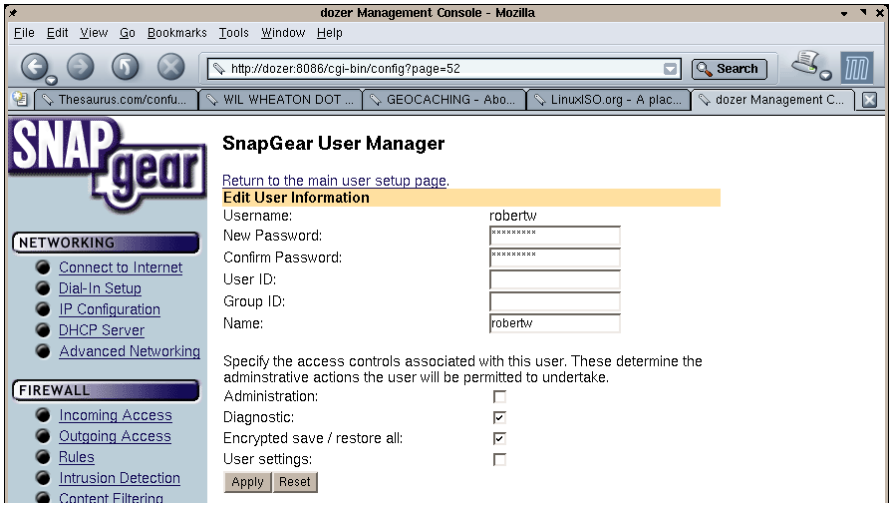



**Figure 9.2 Edit user information**

## Administration

A user with the administration access control is permitted to edit any configuration file on the SnapGear appliance. It should be given to trusted users who are permitted to configure and reconfigure the unit.

## Diagnostic

The diagnostic access control allows a user to view status reports, the technical support report, the system log and other read only pages. No capability is granted to allow such a user to edit any of the configuration on the SnapGear appliance. This access control can be granted to technical support users so they can attempt to diagnose but not fix any problems which occur.

## Encrypted save/restore all

A user with this access control can dump and restore the entire SnapGear appliance's configuration via the encrypted save and restore option on the **Advanced** page. Such a user cannot edit the configuration nor even see the configuration files themselves. This access control can be allocated to a technician whom you want to be able to restore units to a known good configuration but to whom you do not wish to grant full administration rights.

## User settings

A user with this access control can edit users' login information, create new users and modify access controls for other users. Without this access control, users can only change their own passwords. Because this access control allows a user to edit their own permissions, it is best left such that only the *root* user has it.

The *root* user is special. This user alone has one access control which cannot be removed. The *root* user is always able to edit user settings and thus they can grant themselves any access control if need be. The *root* user also has the capability to set **User ID** and **Group ID** when editing or creating users. It is best to leave these fields blank when creating a new user as this lets the SnapGear appliance automatically allocate and manage them.

If somebody with the user settings access control attempts to edit the *root* user (apart from *root* themselves), they must enter the administrative password (i.e. the password for the *root* account).

Finally, the *root* user is the only user permitted to telnet to a SnapGear appliance.

## Password

The SnapGear appliance's administrative (*root*) password is used to restrict access to the *SnapGear Management Console* web administration pages (**Web Admin**) and the SnapGear appliance itself. The SnapGear appliance administrative password is the 'key' to the security of your network and must be kept secret. SnapGear recommends choosing a password that is easy for you to remember but hard for unauthorized people to guess.

A potential security issue may be introduced by having a network-connected SnapGear appliance accessible, using the factory default password. To prevent this, the password for the SnapGear appliance should be changed when Setup Wizard is run or the *SnapGear Management Console* web administration pages are accessed for the first time.

The SnapGear appliance administrative password can be changed at any time using the *SnapGear Management Console* web administration pages by clicking **Password** in the **System** menu.

***Note***

*The username is* **root**. *The factory default SnapGear appliance administrative password is* **default**.

# Diagnostics

If you are experiencing problems with your SnapGear appliance, diagnostic information is provided on the *SnapGear Management Console* web administration pages.

To access this information, from the **System** menu, click **Diagnostics**. Advanced network diagnostics can be viewed by selecting the **Networking** menu, then **Advanced Networking**.

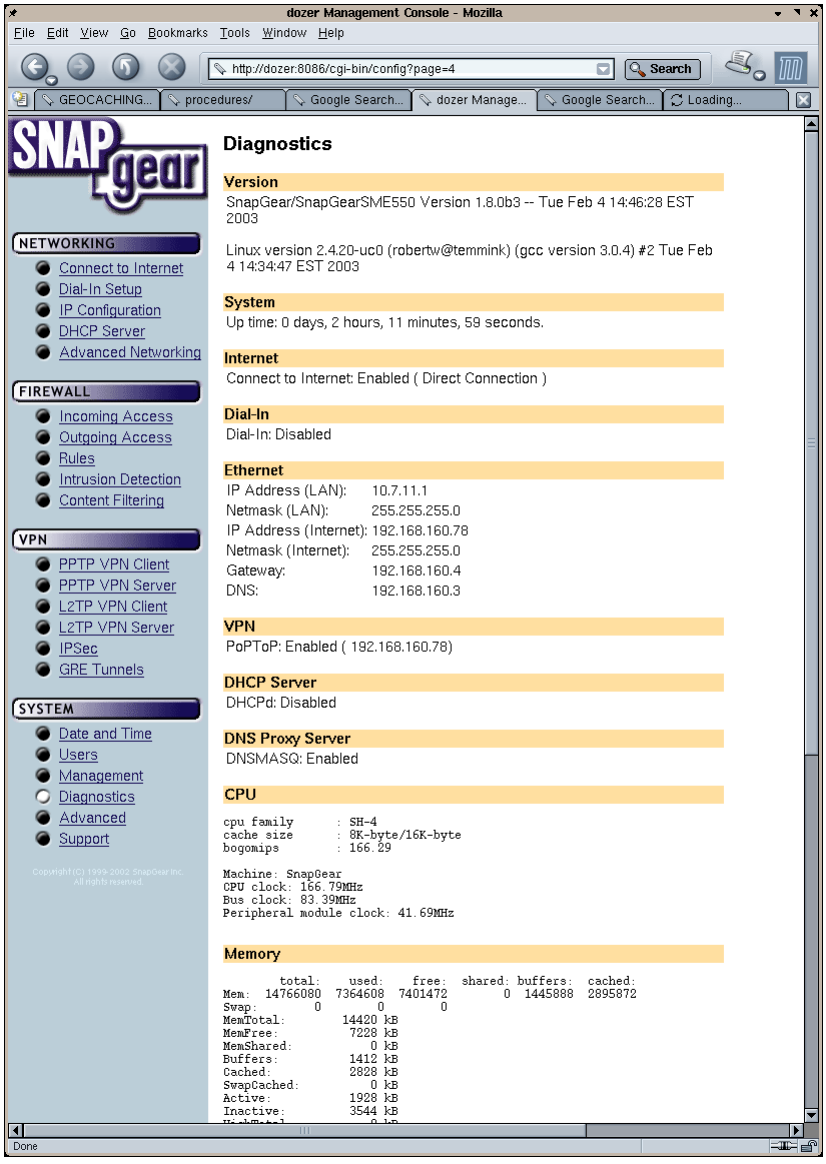



**Figure 9.3 Diagnostics**

# Advanced

The options on the **Advanced** page are intended for network administrators and advanced users **only**.

***Warning***

*Altering the advanced configuration settings may render your SnapGear appliance inoperable.*

## System log

The system log contains debugging information that may be useful in determining whether all services for your SnapGear appliance are operating correctly.

The SnapGear appliance also provides the option of re-directing log output to a remote machine using the syslog protocol. Enable this option by selecting **Enable Remote Logging**, entering the IP address of the remote machine and clicking **Apply**.

Log output is color coded by output type. General information and debug output is black, warnings and notices are blue, and errors are red. The pull down menu underneath the log output allows you to filter the log output to display, based on output type.

Refer to Appendix C for details on configuring and interpreting log output.

## Configuration Files

Clicking **Configuration Files** allows you to select and edit the SnapGear appliance's configuration files manually. Generally, this should only be done at the request of customer support.

The SnapGear appliance's entire configuration may be backed up remotely. Doing this is highly recommended as to minimise downtime in the event of a configuration loss. The configuration may be backed up in plain text, or encrypted with a password.

To backup to a plain text file, click **store/restore** and copy and paste the configuration into a text editor on the remote machine. Restoring is simply a matter of copying and pasting the configuration from the text file back into the same field on the SnapGear appliance and clicking **Submit**.

You may also upload additional configuration files from your computer to the SnapGear appliance under **Upload file**.

To backup to an encrypted file, click save and restore, enter a password and click Save under Save Configuration. To restore from this file, browse for the backup configuration file, enter the password you used to save it and click Restore under Restore configuration.

## Flash upgrade

The SnapGear appliance firmware can be updated with newer versions available from the SnapGear web site (**http://www.snapgear.com/downloads.html**). There are two methods available for performing a flash upgrade.

The first is to download the *netflash.exe* for the appropriate model and version to which you will be upgrading. This is a Windows program that automates the upgrade procedure. Be sure to read the release notes before attempting the upgrade.

The second is to download the binary image file (*.bin*). This can then be transferred from a PC on the local network into the SnapGear appliance's flash memory by way of a TFTP server. This method involves the following steps:

1. Download the appropriate *.bin* file.

2. Start up a TFTP server. Windows users can download a TFTP server program from: **http://www.snapgear.com/ftp/tools/tftpd32j.zip**

   Note that this program is *not* supported by SnapGear, we recommend it however.

   The majority of Linux users will already have a TFTP server installed as part of their distribution, which must be configured and running.

3. In the *SnapGear Management Console* web administration pages, click **Advanced** then **Flash Upgrade**. Enter the server **IP Address** (i.e. PC with the TFTP server and binary image) and the binary image's filename.

4. Click **Upgrade** to commence the upgrade.

During the upgrade, the front panel LEDs on the SnapGear appliance will flash in an in-and-out pattern. The SnapGear appliance retains its configuration information with the new firmware.

***Warning***

*If the flash upgrade is interrupted (e.g. power down), the SnapGear appliance will stop functioning and will be unusable until its flash is reprogrammed at the factory or a recovery boot is performed. User care is advised.*

## Reboot

Clicking this link will cause the SnapGear appliance to perform a soft reboot. It will usually take around 10 seconds before it is up and running again. Note that if you have enabled bridging, the SnapGear appliance may take up to 30 seconds to reboot.

## Reset button

The simplest method to clear the SnapGear appliance's stored configuration information is by pushing the reset button on the back panel of the SnapGear appliance. A bent paper clip is a suitable tool for performing this procedure.

Pushing the reset button clears all stored configuration information, reverts all settings to the factory defaults, and reboots the SnapGear appliance. Note that by default, the SnapGear appliance is *not* configured with an IP address.

It is also possible to clear all stored configuration information and reset the SnapGear appliance so it reboots configured with an IP address. This is done by pressing the reset button twice within 3 seconds. When the SnapGear appliance reboots, it will be configured with the IP address of 192.168.0.1, netmask 255.255.255.0.

# 10. Technical support

The System menu contains an option detailing support information for your SnapGear appliance.

This page provides basic troubleshooting tips, contact details for SnapGear Support, and links to the SnapGear Knowledge Base as shown in the following figure:

Web Page Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History Links
SNAPgear
NETWORKING
Connect to Internet
Dial In Setup
IP Configuration
DHCP Server
Advanced Networking
FIREWALL
Technical Support
Here are some easy options for gaining technical support:
1. Make sure that you have the latest firmware. New firmware is made available regularly be sure to read the Release Notes for important information about the features of the new firmware and any upgrade issues.
2. Please try the Knowledge Base. Many common problems can be solved here.
3. Have you tried searching the site? The search will look in the Knowledge Base and other areas of the site.
4. If your question is not answered here then please try contacting your reseller, or if you bought directly from SnapGear then submit an e-mail to support@snapgear.com and attach the SnapGearSOHO+'s Technical Support Report.
5. In the USA you may call 801-282-8498 between 9am and 5pm MST.
6. In Asia/Pacific you may call 617-34352888 between 9am and 5pm Australia EST.
Internet

**Figure 10.1 Technical support**

The **Technical Support Report** page is an invaluable resource for the SnapGear Technical Support Staff to analyze problems with your SnapGear appliance. The information on this page gives the Support Staff important information about any problems you may be experiencing.

If you experience a fault with your SnapGear appliance, please attach the **Technical Support Report** to your support request.

# Appendix A – LED status patterns

The following table shows the different LED illumination combinations that can indicate possible error conditions.

In each case, the LEDs indicated will be on and steady, unless otherwise noted, and all other LEDs will be off. The Power and System LEDs are not part of the LEDs indicating status. Where the action indicates that you should contact your dealer, please note the LED pattern to assist with faster response and recovery action.

| **LED Pattern** | **Status** | **Action** |
|---|---|---|
| VPN | Memory failure. | Please contact your dealer. |
| COM2 | Console device cannot initialize. | Please contact your dealer. |
| All LEDs on | In recovery mode, usually from a bad Flash image. While the reset button is held in this will be the LED pattern. | |
| VPN and Internet Link | Cannot load static data into memory, probably memory and/or Flash problem. | Please contact your dealer. |
| COM2 and Internet Link | Cannot load SBSS, probably memory and/or Flash problem. | Please contact your dealer. |

# Appendix B – Terminology

This section explains terms that are commonly used in this document.

| Term | Meaning |
|---|---|
| ADSL | Asymmetric Digital Subscriber Line. A technology allowing high-speed data transfer over existing telephone lines. ADSL supports data rates between 1.5 and 9 Mb/s when receiving data and between 16 and 640 Kb/s when sending data. |
| Advanced Encryption Standard (AES) | The Advanced Encryption Standard is a new block cipher standard to replace DES, developed by NIST, the US National Institute of Standards and Technology. AES ciphers use a 128-bit block and 128, 192 or 256-bit keys. The larger block size helps resist birthday attacks while the large key size prevents brute force attacks. |
| Aggressive Mode | This Phase 1 keying mode automatically exchanges encryption and authentication keys and uses less messages in the exchange when compared to Main mode. Aggressive mode is typically used to allow parties that are configured with a dynamic IP address and a preshared secret to connect or if the SnapGear appliance or the remote party is behind a NAT device. |
| Authentication | Authentication is the technique by which a process verifies that its communication partner is who it is supposed to be and not an imposter. Authentication confirms that data is sent to the intended recipient and assures the recipient that the data originated from the expected sender and has not been altered on route. |
| Automatic Keying, Internet Key Exchange (IKE) | This type of keying automatically exchanges encryption and authentication keys and replaces them periodically. |
| Block cipher | A method of encrypting text (to produce ciphertext) in which a cryptographic key and algorithm are applied to a block of data (for example, 64 contiguous bits) at once as a group rather than to one bit at a time. DES, 3DES and AES are all block ciphers. |
| BOOTP | Bootstrap Protocol. A protocol that allows a network user to automatically receive an IP address and have an operating system boot without user interaction. BOOTP is the basis for the more advanced DHCP. |
| CA Certificate | A self-signed certification authority (CA) certificate that identifies a CA. It is called a CA certificate because it is the certificate for the root CA. |

| | |
|---|---|
| Certificates | A digitally signed statement that contains information about an entity and the entity's public key, thus binding these two pieces of information together. A certificate is issued by a trusted organization (or entity) called a Certification Authority (CA) after the CA has verified that the entity is who it says it is. |
| Certificate Authority | A Certificate Authority is a trusted third party, which certifies public key's to truly belong to their claimed owners. It is a key part of any Public Key Infrastructure, since it allows users to trust that a given public key is the one they wish to use, either to send a private message to its owner or to verify the signature on a message sent by that owner. |
| Control Revocation List | A list of certificates that have been revoked by the CA before they expired. This may be necessary if the private key certificate has been compromised or if the holder of the certificate is to be denied the ability to establish a tunnel to the SnapGear appliance. |
| Data Encryption Standard (DES) | The Data Encryption Standard is a block cipher with 64-bit blocks and a 56-bit key. |
| Dead Peer Detection | The method of detecting if the remote party has a stale set of keys and if the tunnel requires rekeying. To interoperate with the SnapGear appliance, it must conform to the draft draft-ietf-ipsec-dpd-00.txt |
| DHCP | Dynamic Host Configuration Protocol. A communications protocol that assigns IP addresses to computers when they are connected to the network. |
| Diffie-Hellman Group or Oakley Group | The groups used as the basis of Diffie-Hellman key exchange in the Oakley protocol, and in IKE. |
| Diffie-Hellman Key Exchange | A protocol that allows two parties without any initial shared secret to create one in a manner immune to eavesdropping. Once they have done this, they can communicate privately by using that shared secret as a key for a block cipher or as the basis for key exchange. |
| Distinguished Name | A list of attributes that defines the description of the certificate. These attributes include: country, state, locality, organization, organizational unit and common name. |
| DNS | Domain Name System that allocates Internet domain names and translates them into IP addresses. A domain name is a meaningful and easy to remember name for an IP address. |
| DUN | Dial Up Networking. |
| Encapsulating Security Payload (ESP) | Encapsulated Security Payload is the IPSec protocol which provides encryption and can also provide authentication service. |
| Encryption | The technique for converting a readable message (plaintext) into apparently random material (ciphertext) which cannot be read if intercepted. The proper decryption key is required to read the message. |
| Ethernet | A physical layer protocol based upon IEEE standards. |

| | |
|---|---|
| Extranet | A private network that uses the public Internet to securely share business information and operations with suppliers, vendors, partners, customers, or other businesses. Extranets add external parties to a company's intranet. |
| Failover | A method for detecting that the main Internet connection (usually a broadband connection) has failed and the SnapGear apliance cannot communicate with the Internet. If this occurs, the SnapGear appliance automatically moves to a lower speed, secondary Internet connection. |
| Fall-forward | A method for shutting down the failover connection when the main Internet connection can be re-established. |
| Firewall | A network gateway device that protects a private network from users on other networks. A firewall is usually installed to allow users on an intranet access to the public Internet without allowing public Internet users access to the intranet. |
| Gateway | A machine that provides a route (or pathway) to the outside world. |
| Hashes | A code, calculated based on the contents of a message. This code should have the property that it is extremely difficult to construct a message so that its Hash comes to a specific value.Hashes are useful because they can be attached to a message, and demonstrate that it has not been modified. If a message were to be modified, then its hash would have changed, and would no longer match the original hash value. |
| Hub | A network device that allows more than one computer to be connected as a LAN, usually using UTP cabling. |
| IDB | Intruder Detection and Blocking. A feature of your SnapGear VPN appliance that detects connection attempts from intruders and can also optionally block all further connection attempts from the intruder's machine. |
| Internet | A worldwide system of computer networks - a public, cooperative, and self-sustaining network of networks accessible to hundreds of millions of people worldwide. The Internet is technically distinguished because it uses the TCP/IP set of protocols. |
| Intranet | A private TCP/IP network within an enterprise. |
| IP Compression | A good encryption algorithm produces ciphertext that is evenly distributed. This makes it difficult to compress. If one wishes to compress the data it must be done prior to encrypting. The IPcomp header provides for this. One of the problems of tunnel mode is that it adds 20 bytes of IP header, plus 28 bytes of ESP overhead to each packet. This can cause large packets to be fragmented. Compressing the packet first may make it small enough to avoid this fragmentation. |
| IPSec | Internet Protocol Security. IPSec provides interoperable, high quality, cryptographically-based security at the IP layer and offers protection for network communications. |
| IPSec tunnel | The IPSec connection to securely link two private parties across insecure and public channels. |

| | |
|---|---|
| IPSec with Dynamic DNS | Dynamic DNS can be run on the IPSec endpoints thereby creating an IPSec tunnel using dynamic IP addresses. |
| IKE | IKE is a profile of ISAKMP that is for use by IPsec. It is often called simply IKE. IKE creates a private, authenticated key management channel. Using that channel, two peers can communicate, arranging for sessions keys to be generated for AH, ESP or IPcomp. The channel is used for the peers to agree on the encryption, authentication and compression algorithms that will be used. The traffic to which the policies will applied is also agreed upon. |
| ISAKMP | ISAKMP is a framework for doing Security Association Key Management. It can, in theory, be used to produce session keys for many different systems, not just IPsec. |
| Key lifetimes | The length of time before keys are renegotiated. |
| LAN | Local Area Network. |
| LED | Light-Emitting Diode. |
| Local Private Key Certificate & Passphrase | The private part of the public/private key pair of the certificate resides on the SnapGear appliance. The passphrase is a key that can be used to lock and unlock the information in the private key certificate. |
| Local Public Key Certificate | The public part of the public/private key pair of the certificate resides on the SnapGear appliance and is used to authenticate against the CA certificate. |
| MAC address | The hardware address of an Ethernet interface. It is a 48-bit number usually written as a series of 6 hexadecimal octets, e.g. 00:d0:cf:00:5b:da. A SnapGear appliance has a MAC address for each Ethernet interface. These are listed on a label on the underneath of the device. |
| Main Mode | This Phase 1 keying mode automatically exchanges encryption and authentication keys and protects the identities of the parties attempting to establish the tunnel. |
| Manual Keying | This type of keying requires the encryption and authentication keys to be specified. |
| Manual Keys | Predetermined encryption and authentication keys used to establish the tunnel. |
| Masquerade | The process when a gateway on a local network modifies outgoing packets by replacing the source address of the packets with its own IP address. All IP traffic originating from the local network appears to come from the gateway itself and not the machines on the local network. |
| MD5 | Message Digest Algorithm Five is a 128 bit hash. It is one of two message digest algorithms available in IPSec. |
| NAT | Network Address Translation. The translation of an IP address used on one network to an IP address on another network. Masquerading is one particular form of NAT. |

| | |
|---|---|
| Net mask | The way that computers know which part of a TCP/IP address refers to the network, and which part refers to the host range. |
| NTP | Network Time Protocol (NTP) used to synchronize clock times in a network of computers. |
| Oakley Group | See Diffie-Hellman Group or Oakley Group. |
| PAT | Port Address Translation. The translation of a port number used on one network to a port number on another network. |
| PEM, DER, PCKS#12 PCKS#07 | These are all certificate formats. |
| Perfect Forward Secrecy | A property of systems such as Diffie-Hellman key exchange which use a long-term key (such as the shared secret in IKE) and generate short-term keys as required. If an attacker who acquires the long-term key provably can neither read previous messages which he may have archived nor read future messages without performing additional successful attacksthen the system has PFS. The attacker needs the short-term keys in order to read the traffic and merely having the long-term key does not allow him to infer those. Of course, it may allow him to conduct another attack (such as man-in-the-middle) which gives him some short-term keys, but he does not automatically get them just by acquiring the long-term key. |
| Phase 1 | Sets up a secure communications channel to establish the encrypted tunnel in IPSec. |
| Phase 2 | Sets up the encrypted tunnel in IPSec. |
| PPP | Point-to-Point Protocol. A networking protocol for establishing simple links between two peers. |
| PPPoE | Point to Point Protocol over Ethernet. A protocol for connecting users on an Ethernet to the Internet using a common broadband medium (e.g. single DSL line, wireless device, cable modem, etc). |
| PPTP | Point to Point Tunneling Protocol. A protocol developed by Microsoft™ that is popular for VPN applications. Although not considered as secure as IPSec, PPP is considered "good enough" technology. Microsoft has addressed many flaws in the original implementation. |
| Preshared secret | A common secret (passphrase) that is shared between the two parties. |
| Quick Mode | This Phase 2 keying mode automatically exchanges encryption and authentication keys that actually establishes the encrypted tunnel. |
| Rekeying | The process of renegotiating a new set of keys for encryption and authentication. |
| Road warrior | A remote machine with no fixed IP address. |
| Router | A network device that moves packets of data. A router differs from hubs and switches because it is "intelligent" and can route packets to their final destination. |

| | |
|---|---|
| RSA Digital Signatures | A public/private RSA key pair used for authentication. The SnapGear appliance can generate these key pairs. The public keys need to be exchanged between the two parties in order to configure the tunnel. |
| SHA | Secure Hash Algorithm, a 160 bit hash. It is one of two message digest algorithms available in IPSec. |
| Security Parameter Index (SPI) | Security Parameter Index, an index used within IPsec to keep connections distinct. Without the SPI, two connections to the same gateway using the same protocol could not be distinguished. |
| Subnet mask | See "Net mask". |
| Switch | A network device that is similar to a hub, but much smarter. Although not a full router, a switch partically understands how to route Internet packets. A switch increases LAN efficiency by utilizing bandwidth more effectively. |
| TCP/IP | Transmission Control Protocol/Internet Protocol. The basic protocol for Internet communication. |
| TCP/IP address | Fundamental Internet addressing method that uses the form nnn.nnn.nnn.nnn. |
| TripleDES (3DES) | Using three DES encryptions on a single data block, with at least two different keys, to get higher security than is available from a single DES pass. |
| UTC | Coordinated Universal Time. |
| UTP | Unshielded Twisted Pair cabling. A type of Ethernet cable that can operate up to 100Mb/s. Also known as Category 5 or CAT 5. |
| VPN | Virtual Private Networking. When two locations commmunicate securely and effectively across a public network (e.g. the Internet). The three key features of VPN technology are privacy (nobody can see what you are communicating), authentication (you know who you are communicating with), and integrity (nobody can tamper with your messages/data). |
| WAN | Wide Area Network. |
| WINS | Windows Internet Naming Service that manages the association of workstation names and locations with IP addresses. |
| x.509 Certificates | An x.509 certificate includes the format of the certificate, the serial number of the certificate, the algorithm used to sign the certificate, the name of the CA that issued the certificate, the name and public key of the entity requesting the certificate, and the CA's signature.x.509 certificates are used to authenticate the remote party against a Certificate Authority's (CA) certificate. The CA certificate must have signed the local certificates that are used for tunnel authentication. Certificates need to be uploaded into the SnapGear before a tunnel can be configured to use them (see Certificate Management). |

# Appendix C – System Log

## Access Logging

It is possible to log any traffic that arrives at or traverses the SnapGear appliance. The only logging that is enabled by default is to take note of packets that were dropped. While it is possible to specifically log exactly which rule led to such a drop, this is not configured by default. All rules in the default security policy drop packets. They never reject them. That is, the packets are simply ignored, and have no responses at all returned to the sender. It is possible to configure reject rules if so desired.

All traffic logging performed on the SnapGear appliance creates entries in the syslog (*/var/log/messages* - or external syslog server) of the following format:

*<Date/Time>* **klogd:** *<prefix>* **IN=***<incoming interface>* **OUT=***<outgoing interface>* **MAC=***<dst/src MAC addresses>* **SRC=***<source IP>* **DST=***<destination IP>* **SPT=***<source port>* **DPT=***<destination port>* *<additional packet info>*

Where:

| | |
|---|---|
| **<prefix>** | if non-empty, hints at cause for log entry |
| **<incoming interface>** | will be empty, or one of eth0, eth1 and similar |
| **<outgoing interface>** | as per incoming interface |
| **<dst/src MAC addresses>** | MAC addresses associated with the packet |
| **<source IP>** | packet claims it came from this IP address |
| **<destination IP>** | packet claims it should go to this IP address |
| **<source port>** | packet claims it came from this TCP port |
| **<destination port>** | packet wants to go to this TCP port |

Depending on the type of packet and logging performed some of the fields may not appear.

Commonly used interfaces are:

| | |
|---|---|
| **eth0** | the LAN port |
| **eth1** | the WAN/Internet port |
| **ppp*X*** | e.g. *ppp0* or *ppp1* – a PPP session |
| **ipsec*X*** | e.g. *ipsec0*, an IPSec interface |

The firewall rules deny all packets arriving from the WAN port by default. There are a few ports open to deal with traffic such as DHCP, VPN services and similar. Any traffic that does not match the exceptions however is dropped.

There are also some specific rules to detect various attacks (smurf, teardrop, etc.).

When outbound traffic (from LAN to WAN) is blocked by custom rules configured in the GUI, the resultant dropped packets are also logged.

The <*prefix*> for all these rules is varied according to their type.

Currently used prefixes for traffic arriving:

| | |
|---|---|
| **Default Deny** | Packet didn't match any rule – drop it |
| **Invalid** | Invalid packet format detected |
| **Smurf** | Smurf attack detected |
| **Spoof** | Invalid IP address detected |
| **SynFlood** | SynFlood attack detected |
| **Custom** | Custom rule dropped outbound packet |

A typical *Default Deny:* will thus look similar to the following:

```
Mar 27 09:31:19 2003 klogd: Default deny: IN=eth1
OUT=MAC=00:d0:cf:00:ff:01:00:e0:29:65:af:e9:08:00
SRC=140.103.74.181 DST=12.16.16.36 LEN=60 TOS=0x10 PREC=0x00
TTL=64 ID=46341 DF PROTO=TCP SPT=46111 DPT=139 WINDOW=5840
RES=0x00 SYN URGP=0
```

That is, a packet arriving from the WAN (*IN=eth1*) and bound for the SnapGear appliance itself (*OUT=<nothing>*) from IP address 140.103.74.181 (*SRC=140.103.74.181*), attempting to go to port 139 (*DPT=139*, Windows file sharing) was dropped.

If the packet is traversing the SnapGear appliance to a server on the private network, the outgoing interface will be eth0, e.g.:

```
Mar 27 09:52:59 2003 klogd: IN=eth1 OUT=eth0 SRC=140.103.74.181
DST=10.0.0.2 LEN=60 TOS=0x10 PREC=0x00 TTL=62 ID=51683 DF
PROTO=TCP SPT=47044 DPT=22 WINDOW=5840 RES=0x00 SYN URGP=0
```

Packets going from the private network to the public come in eth0, and out eth1, e.g.:

```
Mar 27 10:02:51 2003 klogd: IN=eth0 OUT=eth1 SRC=10.0.0.2
DST=140.103.74.181 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=62830 DF
PROTO=TCP SPT=46486 DPT=22 WINDOW=5840 RES=0x00 SYN URGP=0
```

## Creating Custom Log Rules

Additional log rules can be configured to provide more detail if desired. For example, by analyzing the rules in the **Rules** menu, it is possible to provide additional log messages with configurable prefixes (i.e. other than *Default Deny:*) for some allowed or denied protocols.

Depending on how the *LOG* rules are constructed it may be possible to differentiate between inbound (from WAN to LAN) and outbound (from LAN to WAN) traffic. Similarly, traffic attempting to access services on the SnapGear appliance itself can be differentiated from traffic trying to pass through it.

The examples below can be entered on the Command Line Interface (telnet), or into the **Rules** SnapGear Management Console web administration pages. Rules entered on the CLI are not permanent however, so while it may be useful for some quick testing, it is something to be wary of.

To log permitted inbound access requests to services hosted on the SnapGear appliance, the rule should look something like this:

**iptables -I INPUT -j LOG -p tcp --syn -s** *<X.X.X.X/XX>* **-d** *<Y.Y.Y.Y/YY>* **--dport** *<Z>* **--log-prefix** *<prefix>*

This will log any TCP (*-p tcp*) session initiations (*--syn*) that arrive from the IP address/netmask *X.X.X.X/XX* (*-s ...*) and are going to *Y.Y.Y.Y/YY*, destination port Z (*--dport*).

For example, to log all inbound access requests from anywhere on the Internet (0.0.0.0/0) to the PPTP service (port 1723) on the SnapGear appliance (IP address 1.2.3.4):

```
iptables -I INPUT -j LOG -p tcp --syn -s 0.0.0.0/0 -d 1.2.3.4
--dport 1723 --log-prefix "Internet PPTP access: "
```

To find the resultant log entry in the logs, simply search for the prefix, in this instance *"Internet PPTP access: "*.

If for example site 192.0.1.2 attempted to access the SnapGear appliance's PPTP port, the resultant log message would look something like this:

```
<12> Jan 24 17:19:17 2000 klogd: Internet PPTP access: IN=eth0
OUT= MAC=00:d0:cf:00:07:03:00:50:bf:20:66:4d:08:00 SRC=
DST=1.2.3.4 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=43470 DF
PROTO=TCP SPT=4508 DPT=1723 WINDOW=64240 RES=0x00 SYN URGP=0
```

Note how *OUT* is set to nothing. This indicates that the packet was attempting to reach a service on the SnapGear appliance, rather than attempting to pass through it.

A very similar scenario occurs for logging access requests that are attempting to pass through the SnapGear appliance. It merely requires replacing the *INPUT* keyword with *FORWARD*.

Thus, to log permitted inbound requests to services hosted on a server behind the SnapGear appliance, or outbound requests to services on a public network server, use:

**iptables -I FORWARD -j LOG -p tcp --syn -s** *<X.X.X.X/XX>* **-d** *<Y.Y.Y.Y/YY>* **--dport** *<Z>* **--log-prefix** *<prefix>*

For example, to log all inbound requests from the IP address 5.6.7.8 to the mail server (port 25) on the machine *flubber* on the LAN with address 192.168.1.1:

```
iptables -I FORWARD -j LOG -p tcp --syn -s 5.6.7.8/32 -d
192.168.1.1 --dport 25 --log-prefix "Mail for flubber: "
```

This will result in log output something like this:

```
<12> Jan 24 18:17:19 2000 klogd: Mail for flubber: IN=eth1
OUT=eth0 SRC=5.6.7.8 DST=192.168.1.1 LEN=48 TOS=0x00 PREC=0x00
TTL=126 ID=45507 DF PROTO=TCP SPT=4088 DPT=25 WINDOW=64240
RES=0x00 SYN URGP=0
```

Note how the *OUT* value has now changed to show which interface the access attempt will use to reach the internal host. As this request arrived on eth1 and was destined for eth0, we can determine that it was an *inbound* request, since eth0 is the LAN port, and eth1 is usually the WAN port.

An *outbound* request would have *IN=eth0* and *OUT=eth1*.

It is possible to use the *-i* and *-o* arguments to specify the interface that are to be considered for *IN* and *OUT* respectively. When the *!* argument is used before the interface name, the sense is inverted. If the name ends in a **+**, then any interface which begins with this name will match. e.g.

```
iptables -I FORWARD -j LOG -i eth0 -p tcp ...
```

This rule will log outbound from the LAN (eth0) only. We could limit that further by specifying which interface it is outbound to, by using the *-o* option.

```
iptables -I FORWARD -j LOG -i eth0 -o eth1 -p tcp ...
```

This will log LAN traffic destined for the WAN – but won't log LAN traffic destined for a PPP or perhaps IPSec link.

Similarly, we could construct a rule that looks at all inbound/outbound traffic, but excludes VPN traffic, thus:

```
iptables -I FORWARD -j LOG -i eth+ -o eth+ -p tcp ...
```

If we just wanted to look at traffic that went out to the IPSec world, we could use:

```
iptables -I FORWARD -j LOG -o ipsec+
```

Clearly there are many more combinations possible.

It is therefore possible to write rules that log inbound and outbound traffic, or to construct several rules that differentiate between the two.

## Rate Limiting

*iptables* has the facility for rate-limiting the log messages that are generated, in order to avoid denial of service issues arising out of logging these access attempts. To achieve this, use the following option:

**--limit** *rate*

> *rate* is the maximum average matching rate, specified as a number with an optional */second*, */minute*, */hour*, or */day* suffix. The default is *3/hour*.

**--limit-burst** *number*

> *number* is the maximum initial number of packets to match. This number gets recharged by one every time the limit specified above is not reached, up to this number. The default is *5*.

*iptables* has many more options. Perform a web search for *manpage iptables* to find the relevant documentation.

The *LOG* rules configured by default (e.g. *Default Deny:*) are all limited to:

```
--limit 3/hour --limit-burst 5
```

## Administrative Access Logging

When a user tries to log onto the SnapGear Management Console web administration pages, one of the following log messages appears:

```
Jan 30 03:00:18 2000 boa: Authentication successful for root from
10.0.0.2
```

```
Jan 30 03:00:14 2000 boa: Authentication attempt failed for root
from 10.0.0.2
```

This message shows the date/time, whether the authentication succeeded or failed, the user attempting authentication (in this case *root*) and the IP address from which the attempt was made.

Telnet (Command Line Interface) login attempts appear as:

```
Jan 30 03:18:37 2000 login: Authentication attempt failed for
root from 10.0.0.2
```

```
Jan 30 03:18:40 2000 login: Authentication successful for root
from 10.0.0.2
```

Once again, showing the same information as a web login attempt.

## Boot Log Messages

The SnapGear appliance's startup boot time messages are identified by log messages similar to the following:

```
klogd: Linux version 2.4.20-uc0 (jamma@daniel) (gcc version
3.0.4) #4 Mon Feb 3 15:17:50 EST 2003
```

This also shows the version of the operating system (linux), and the build date and time.